

**Contents**

1. Introduction p1-4

2. Privacy Policy p5-12

3. Notice of Processing of Personal Data p13-17

4. Processing of Employee Personal Data p18-19

5. Data Sharing p20-22

6. Next Steps p23

Appendix 1 – Model Privacy Policy (13 pages)

Appendix 2 – Data Retention Periods Guidelines (3 pages)

Appendix 3 – Model Fair Processing Notice (6 pages)

Appendix 4 – Personal Data Map (1 page)

Appendix 5 – Model Employee Fair Processing Notice (5 pages)

Appendix 6 – Contract of Employment (Data Protection Clause) (1 page)

Appendix 7 – Model Data Protection Addendum (12 pages)

Appendix 8 – Model Data Sharing Agreement (16 pages)

Appendix 9 - Frequently Asked Questions (18 pages)

**1.** **Introduction**

This document, together with the appended model documentation, was originally prepared in February 2018 for use by you as a member of SFHA/GWSF when updating paperwork and procedures in relation to data protection matters in advance of the implementation of the General Data Protection Regulation (GDPR) – which came into force in May 2018. SFHA and GWSF would like to acknowledge its small working group of members for their extremely helpful contribution to the production of this documentation in 2018.

Since then, legislative changes and questions raised by members have necessitated updates to the guidance, including those relating to the Freedom of Information Act 2002 (FOISA) from 11 November 2019 and Brexit in January 2021. The model documentation and FAQ document appended hereto is designed to assist you in ensuring your data protection documentation is in line with the requirements imposed on you by the GDPR. Nothing contained in these guidance notes or the appended model documentation is to be taken as constituting legal advice in any way, and members are encouraged to take their own independent legal advice in relation to the finalisation of their updated data protection documentation.

A version of the model documentation with changes tracked to the previous 2018 version is available via the link below. This tracks minor changes applied in the October 2019:

[Model Documentation with Changes Tracked to 2018 Version](https://www.sfha.co.uk/download.php?file=1287)

Further minor changes applied to the model documentation in June 2021 are tracked here: [Model Documentation with June 2021 changes tracked](https://www.sfha.co.uk/download.php?file=1649)

* 1. **General Data Protection Regulation (GDPR)**

The GDPR[[1]](#footnote-2) came into force on 25 May 2018. This is a regulation of the European Union and has direct effect in the United Kingdom as it presently stands. The UK GDPR is now in force post-Brexit and through this piece of legislation, the terms of the GDPR apply, with some minor changes and differences.

The GDPR overhauled many areas of data protection laws and replaced the Data Protection Act 1998. The Data Protection Act 2018[[2]](#footnote-3) (“the 2018 Act”) supplements the GDPR and should be implemented alongside it. There were many changes to the legislative framework imposed by the GDPR and the 2018 Act. SFHA/GWSF have worked together alongside TC Young to produce model documentation reflecting the amended legislation that governs data protection in the United Kingdom. All members of SFHA and GWSF are affected by the terms of the GDPR and need to ensure that their documentation is regularly updated and compliant with the terms of the GDPR.

All organisations processing personal data are required to comply with the terms of the GDPR. Such organisations are defined in the GDPR as “Data Controllers”. As a result of your processing of personal data, you are a Data Controller. Furthermore, if you enter into contractual relationships with third parties whom you ask to process personal data on your behalf for various reasons (e.g. if you outsource payroll), the GDPR defines those third-party processors as “Data Processors”. They also are required to comply with the GDPR.

You should consider whether you are in fact a Data Processor on behalf of any other organisation.

**1.2 Changes to Registration Requirements with the ICO**

Under the previous requirements, organisations with fewer than 250 employees paid a data protection fee to the ICO of £35 and organisations with more than 250 employees paid £500. This has now changed, as a result of the Data Protection (Charges and Information) Regulations 2018. The new requirements state that:

* organisations with 10 or fewer staff and charities pay a fee of £40.
* Organisations with between 11 and 250 staff pay £60
* Large organisations with over 250 now pay £2,900.
* Organisations established entirely for not-for-profit making purposes do not have to pay a fee.

All registered Scottish charities, therefore most RSLs, will be required to pay a flat rate of £40 regardless of organisation size. If you are an RSL which is not a registered charity, then the differing registration rates above apply depending on the organisation size.

More guidance on registration is available on the ICO website.[[3]](#footnote-4)

* 1. **Model Documentation**

There are various documents appended to these guidance notes. These comprise the key documentation that you will require to review and most likely update to ensure your organisation remains compliant with the terms of the GDPR. This documentation includes:

* Model Privacy Policy (incorporating Data Retention Guidelines);
* Model Fair Processing Notice;
* A template for Mapping Personal Data
* Model Employee Fair Processing Notice;
* Model Data Protection Clause for Contracts of Employment;
* Model Data Protection Addendum (for use with your data processors); and
* Model Data Sharing Agreement (for use with other data controllers).

This documentation is in model form only and will require to be adjusted to reflect your own organisation’s practices and procedures to ensure that the documentation correctly reflects those practices and procedures. Given the nature of the GDPR and data protection matters, it is impractical to produce a “one size fits all” set of documents that you will be able to adopt as drafted. This is owing to the different activities carried out by individual organisations and the manner in which those activities are carried out.

In recognition that many members will have adopted the previous versions of the model documentation, a version with changes tracked to the previous 2018 documents made in October 2019 is available via the link below:

[Model Documentation with Changes Tracked to 2018 Version](https://www.sfha.co.uk/download.php?file=1287)

Further tracked changes to the model documentation made in June 2021 are available here: [Model Documentation with June 2021 changes tracked](https://www.sfha.co.uk/download.php?file=1649)

* 1. **Guidance Notes and Frequently Asked Questions**

These guidance notes are to be read in conjunction with the attached model documentation. They will assist your organisation in establishing and updating the terms of the necessary documentation you require to have in place in compliance with the GDPR. In addition to these notes, drafting notes have been provided where practicable within the model documentation.

A Frequently Asked Questions document is also included at Appendix 9.

**2. Privacy Policy**

All member organisations will likely have in place a Privacy Policy. This requires to be regularly updated, particularly if any of your organisation’s internal operations, practices or processes change.

The Model Privacy Policy at Appendix 1 sets out both the policy and procedure for you to adopt in compliance with the GDPR. This should be updated to reflect your own practices and day to day activities.

**2.1 Processing of Personal Data - Consent**

It was commonplace under the Data Protection Act 1998 for Data Controllers to heavily rely on a general form of consent obtained by them to process an individual’s personal data. The requirements for obtaining consent are overhauled by the GDPR. Consent can no longer be given in a general sense and must be given freely, to a specific purpose of processing and by an affirmative action (i.e. seeking individuals to opt in rather than opt out). You therefore need to review your existing consent and see whether you need to update and obtain fresh consent in order to ensure that you can process personal data someone has previously consented to you processing.

You need to consider consent as a basis for processing in general and its use where other grounds for processing that personal data are unavailable (see 2.2 Grounds for Obtaining Personal Data Without Obtaining Consent). An example where you will need to consider consent would be in relation to the use of images in any publications or on your website, and a form of wording in that respect will need to be composed to ensure that consent is sought for a specific purpose.

If you are processing personal data obtained from tenant conferences, AGMs or similar events then you will need to obtain consent to process that personal data for each specific use of that data (i.e. a photograph in your newsletter publication/ website).

**2.2 Grounds for Processing Personal Data Without Obtaining Consent**

There are other grounds for processing personal data that should be used where possible rather than obtaining consent. These grounds are:

* Necessary for performance of a contract between organisation and data subject or entering into a contract (e.g. name, date of birth, contact details);
* Necessary for compliance with a legal obligation (e.g. employment related requirements, such as the need to disclose salary details to HMRC);
* Necessary to protect the vital interests of the data subject or another person (e.g. life-threatening situations);
* Necessary for the performance of a task carried out in the public interest or in exercise of an organisation’s official authority (for Public Authorities only).

**2.3 Legitimate Interests**

When FOI legislation was extended to RSLs in November 2019, this had a significant impact on RSLs’ ability to rely on the legitimate interests ground for processing. This is because “public authorities” as defined by the Freedom of Information (Scotland) Act 2002 (FOISA), (which includes RSLs in respect of specified functions from 11 November 2019[[4]](#footnote-5) ) are restricted in their ability to use the legitimate interest ground for processing.

This means that legitimate interests could only potentially be used by RSLs when it concerned matters not in connection with their role as a public authority. As this can be difficult to demonstrate, it is not recommended to use this ground for most day-to-day processing of tenant data and RSLs should think carefully and consider seeking appropriate advice when thinking about using legitimate interests as a processing ground.

As a result, it may feel to many RSLs like you are losing your ‘catch-all’ basis for processing. However, the legitimate interests ground was only ever intended to be used as a last resort and should rarely have been relied on by RSLs. The ICO has made it clear that the most common basis for processing for landlords should be that processing is necessary for the performance of the contract (i.e. the tenancy agreement in the case of RSLs). Therefore, so long as your Privacy Policy and Fair Processing Notice have been appropriately amended, there should be little change to your operations as a result of the loss of the legitimate interests ground.

**2.4 Security**

You require to continue to review your practices in relation to the security of personal data both in paper and electronic format, in order to ensure these practices are updated to reflect current security measures. You need to speak to any I.T. provider you contract with in relation to security issues. The terms of the Model Privacy Policy should be adjusted to reflect your own security requirements.

**2.5 Breaches**

The GDPR imposes a timeframe for reporting breaches which pose a risk to the rights and freedoms of data subjects (individuals). In accordance with the terms of the draft policies, these breaches must be reported to the Information Commissioner’s Office (ICO) within 72 hours of the breach occurring or from the point you become aware of that breach if later.

When you are appointing a statutory Data Protection Officer (see section 2.6) then they will need to ensure they are reporting the breach within that timeframe.

It is important to note that not all breaches need to be reported to the ICO, and it depends on the nature and severity of the breach. The examples below illustrate this difference. Given the infancy of the legislation, we await further, more detailed guidance in relation to reportable and non-reportable breaches.

***Example 1***

*Your Association (the controller) contracts a payroll provider (the processor) which processes the Association’s staff data. The payroll provider detects an attack on its network that results in personal data about your employees being unlawfully accessed. As this is a personal data breach, the payroll provider promptly notifies you that the breach has taken place. The breach is a risk to rights and freedoms as vulnerable data, such as bank details, has been accessed. You in turn notify the ICO. You become aware of the breach at 4.45 pm on a Friday afternoon. You have until 4.45 pm on Monday to report the breach. Given the day and time of being informed, and the intervening weekend, you don’t have enough time to obtain all the relevant details from the payroll provider. However, you report to the ICO anyway within the required time limits and explain that your investigations are still ongoing, with more information to follow.*

***Example 2***

*Your Association issued an email to a list of tenants without realising that all email addresses would show in the list and be seen by all recipients. Some of the email addresses contain personal data (i.e. joe.bloggs@hotmail.com). Some are more generic (i.e. prettyprincess@yahoo.co.uk). The email simply advises of a new Housing Manager being appointed. There is no information in the email which relates directly or indirectly to the tenants. There is no risk to the tenants’ rights and freedoms. The breach should be recorded internally but does not need to be reported to the ICO.*

**2.6 Data Protection Officers (DPO)**

In terms of the GDPR, a DPO requires to be appointed by organisations who are deemed to be a public authority in terms FOISA, or whose core activities involve a large-scale monitoring of individuals or the large-scale processing of sensitive personal data.

As RSLs were classed as public authorities under the terms of FOISA from 11 November 2019, since that date it has been mandatory for RSLs to appoint a DPO.

**2.6.1 Role of the Data Protection Officer**

A DPO can be appointed from within your current workforce or could be contracted in either as a consultant or employee. Broadly, their role is to ensure data protection compliance by the organisation. The Information Commissioner (ICO) provides further guidance on its website regarding DPOs[[5]](#footnote-6), and outlines the following as key tasks that the DPO must undertake:

* to inform and advise you and your employees about your obligations to comply with the GDPR and other data protection laws;
* to monitor compliance with the GDPR and other data protection laws, and with your data protection polices, including managing internal data protection activities; raising awareness of data protection issues, training staff and conducting internal audits;
* to advise on, and to monitor, [data protection impact assessments](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/);
* to cooperate with the supervisory authority (the ICO); and
* to be the first point of contact for supervisory authorities (the ICO) and for individuals whose data is processed (employees, customers etc).

**2.6.2 Appointment of a Data Protection Officer**

There are a number of individuals and organisations who have made themselves available to take on the role of a DPO on a consultancy basis or to provide support to your DPO. If you are exploring this option, you are encouraged to ensure that you discuss your operational activities in detail with any prospective consultant DPO, in order that the consultant can ensure they understand the operational activities of your organisation.

Small to medium sized organisations may consider it more resourceful and economical to outsource DPO services. It is also possible for RSLs to appoint a ‘joint’ DPO if the nature of their operations, structure, and services are similar. Again, the DPO can be an external, outsourced individual.

Regardless of whether the DPO is an internal member of staff or outsourced, they must report to the highest level of management and be given the required autonomy for the purposes of their DPO functions. The DPO cannot be penalised in a personal capacity for the performance of their duties and cannot be given any duties which conflict with their role as DPO.

Every RSL runs its business in a manner which best suits its activities and functions. RSLs will need to consider their specific business structure, reporting lines, and individual roles and duties in order to determine who is best placed to take on the role of the DPO. It should also be noted that the highest level of management (i.e. Director, CEO, governing body members) cannot be appointed as DPOs

When recruiting or sourcing a DPO, it is important to consider the individual’s experience and knowledge of data protection matters and their awareness of your organisation’s operations. This, however, is expected to be proportionate to the size of the organisation which, in turn, should ensure that resources being expended on a DPO are relative to the size of the organisation and its funds.

The FAQs at Appendix 9 further address the DPO requirement (see Questions 40-49).

SFHA has negotiated a package of services for its members at discounted rates, ranging from advisory services for internal DPOs to direct DPO services on a retainer basis. More details are available on the SFHA website here:

[DPO services for SFHA members](https://www.sfha.co.uk/our-work/policy-category/governance-and-regulation/sub-category/data-protection/policy-article/data-protection-officer-services)

**2.7 Rights of Individuals**

The GDPR gives enhanced rights to individuals. Clause 9 of the Model Privacy Policy details those rights. You should note the requirement to comply with tighter timeframes for responding to subject access requests, as well as the new rights to be forgotten, and to restrict or object to processing of data.

**2.7.1 Right of Access (Subject Access Requests)**

Individuals have the right to view personal data held by you about them. This right is probably the most commonly exercised right and is known as a Subject Access Request (SAR), in which an individual will request copies/to review data held about them in relation to specific matters (e.g. ASB complaints made about them).

SARs do not have to be made in writing- even a verbal SAR must be complied with. A SAR must be dealt with no later than one month from the day after the request was made. The examples below show how this time limit is applied in practice:

***Example 3***

*An organisation receives a request on 3 September. The time limit will start from the next day (4 September). This gives the organisation until 4 October to comply with the request.*

***Example 4***

*An organisation receives a request on 30 March. The time limit starts from the next day (31 March). As there is no equivalent date in April, the organisation has until 30 April to comply with the request. If 30 April falls on a weekend, or is a public holiday, the organisation has until the end of the next working day to comply.*

Under the GDPR, data subjects are entitled to only the data held about them. Of course, when it comes to housing files, it will not be uncommon for other tenants to be referenced. Where third parties can be identified from the data, the Association must make reasonable attempts to obtain those third parties’ consent for disclosure. Where there is no consent, the Association must consider whether it would be reasonable to disclose the third-party references anyway. If it would not be reasonable, the Association must redact references to third parties from the data being supplied to the data subject making the SAR.

Associations can no longer charge data subjects except where the administrative costs of complying with the SAR are manifestly unfounded, excessive, or repeated. An example (provided by the ICO) of a request which is manifestly unfounded is included below.

***Example 5***

*An individual believes that information held about them is inaccurate. They repeatedly request its correction but you have previously investigated and told them you regard it as accurate. The individual continues to make requests along with unsubstantiated claims against you as the controller. You refuse the most recent request because it is manifestly unfounded and you notify the individual of this.*

**2.8 Data Retention**

The model documentation includes Data Retention Guidelines (see Appendix 2) – which are for guidance only. It is recommended that you do not arbitrarily fix set retention periods, which you are then bound to ensure compliance with. These can be amended by you, but you should ensure that you have a justification for the retention periods referred to, and that the data is retained only in connection with the original purpose for which it was collected for processing.

The National Housing Federation also provides guidance on document retention available on its website.[[6]](#footnote-7)

The Scottish Council on Archives also provides some further examples of retention schedules, including one specifically relating to housing.[[7]](#footnote-8)

It is important note that – under data protection legislation – there is no set format in which documents must be retained. This means there is no explicit requirement, in terms of data protection, to retain a hard copy if you are retaining electronically – but you may wish to consider doing so if you wish an additional back up. You should also consider any relevant polices and other legal and/or regulatory requirements where determining if hard copy documents require retention.

**2.9 Access to the policy**

It is recommended that you make your privacy policy available online and in hard copy form within your offices.

**3. Notice of Processing of Personal Data**

The GDPR imposes a requirement for each Data Controller to provide documentation which notifies individuals what personal data of theirs is processed by you. This takes the form of a Fair Processing Notice (FPN) – sometimes referred to as a Privacy Notice. This must be a stand-alone document which is easy to access, intelligible and written in plain English. Previously, an FPN was commonly included within an organisation’s data protection or privacy policy. Given the new requirements to have this as a stand-alone document, the model documentation includes a Model FPN at Appendix 3.

**3.1 Model Fair Processing Notice**

The model FPN is designed for use when processing personal data of external individuals (i.e. tenants, factored owners, board members etc.).

The FPN must contain details of the following:

* Identity and contact details of the Data Controller;
* Data processing purpose and basis;
* Recipients of the data;
* Details of any transfer of the data out with the EU and the protections in place;
* How long the data will be held, or if unknown then how the data controller will determine how long it is to be held;
* Information on whether the data will be processed as part of an automated decision-making process and the consequences of such processing;
* The contact details of your appointed DPO;
* Information on the data subject’s rights including the consequences of their failure to provide such data where required by statute or contract; and
* Any further information which is not already covered by the above.

**3.2 How to use the FPN**

The FPN must be provided to individuals whose personal data is collected at the outset of the collection of that data by your organisation. It will therefore mean that you will need to develop procedures to ensure that the notice is included within any application packs if you take in applications for tenancies, by way of example, and process the personal data contained within those applications. Further, it is recommended that you also provide a copy of the FPN to all new tenants/factored owners.

You are required to ensure that you have provided a copy of this FPN, however you are under no obligation to ensure that any individual the notice has been provided to, and whose personal data you are processing, has read that document. The FPN therefore does not require to be signed.

**3.3 How to complete the FPN**

Drafting notes have been included at the beginning of each section of the model FPN. These should be reviewed when finalising the terms of your FPN. You should carry out a departmental audit of personal data held, consulting and updating the Personal Data Map (see Appendix 4).

**3.3.1 Personal Data**

The personal data you process should be clearly narrated within the FPN.

The Personal Data Map at Appendix 4 should be used when carrying out your internal audit of personal data you hold. It should be completed on a departmental basis and that information collated. Once that exercise has been carried out you can proceed to finalise the terms of your FPN.

**3.3.2 Special Categories of Personal Data (Sensitive Personal Data)**

You must identify 2 grounds from separate lists in order to lawfully process sensitive personal data. The first ground will be from the same list as grounds for processing regular personal data (see 2.1 and 2.2). The second ground will be from a separate list of specific grounds which apply to just sensitive personal data. The sensitive personal data grounds include the following:

* Explicit Consent for specific purpose;
* Necessary to comply with obligations re employment or social security;
* Necessary to protect vital interests of the data subject;
* Necessary for the establishment of, exercise or defence of legal claims;
* Necessary for reasons of substantial public interest (this basis is limited and further advice should be sought if exploring this option).

You will need to review what sensitive personal data you process, and why you process that data. Those who provide a care or support facility/service will need to consider this in far greater detail as well. It is likely that the amount of sensitive personal data you hold if you are providing care facilities such as a sheltered housing complex will be voluminous. You will need to consider why you require that information, how it is stored and who has access to it.

**3.3.3 Location of Data**

You will need to review where the personal data you process is held. If any data is transferred to countries outside of the European Union, then you will need to look very closely at the safeguards you need to have in place in order to be compliant with the terms of the GDPR.

In order to be GDPR compliant, personal data cannot be transferred to countries out-with the European Union unless:

* The recipient country has been granted ‘adequacy status’ by the European Commission
* There is an appropriate safeguard in place between the Data Controller and recipient
* Any of the GDPR exemptions apply

**3.3.4 Data Protection Officer**

There is reference to a Data Protection Officer (DPO) within the terms of the FPN. Once a DPO is appointed in advance of 11 November 2019, you must ensure that their name and contact details are narrated within the FPN.

**3.4 Marketing**

Direct marketing is the communication (by whatever means) of advertising or marketing material which is directed to particular individuals. The ICO is yet to produce its final Direct Marketing code, but has made clear whilst consulting on this guidance[[8]](#footnote-9) that direct marketing includes fundraising activities by a charitable organisation.

If your Association is engaged in any form of direct marketing, then you should include reference to this within your FPN. The wording below could be included within your FPN if you are involved in direct marketing:

***Marketing***

*From time to time we would like to contact you with details of other products/ services we provide. You have a choice about whether or not you wish to receive this information from us.*

If you are involved in any form of direct marketing, then you should seek written consent from individuals. An example of the consent form is set out below:

*We have products/ services that we would like to tell you about. If you consent to us contacting you for this purpose please tick to say how you would like us to contact you:*

***Post*** *☐****Email*** *☐* ***Telephone****☐****Text message****☐* ***Automated call****☐*

*If at any time you change your mind about being contacted in the future by any of these means then please let us know by contacting #.*

**3.4.1 Newsletters**

A number of members have queried whether your standard issue tenant newsletters would constitute marketing. From the information provided in relation to these newsletters, it would not seem to be the case that these newsletters would be deemed to constitute marketing, and therefore specific consent to continue to distribute these newsletters directly to members etc. is not required.

However, if the newsletters contain photographs from events then you should ensure that you are obtaining individuals’ consent to use those photographs in that newsletter publication, ensuring that specific consent is obtained from the individuals. Please note that this is only necessary where individuals are “identifiable” and not where photographs of unidentifiable crowds are taken. “Identifiable” in this context means that an individual’s facial features can be seen to the extent of distinguishing them from someone else.

Questions 26-39 of the FAQs at Appendix 9 also address Newsletters and Photographs.

**4. Processing of Employee Personal Data**

Employee information also requires to be processed in accordance with the terms of the GDPR. You will therefore need to have a document which is in effect an employee Fair Processing Notice available to employees/prospective employees to detail what personal data of theirs is processed by the organisation.

**4.1 Employee Fair Processing Notice**

A separate Model Fair Processing Notice has been produced for use in connection with your use of employee information (see Appendix 5). The Fair Processing Notice for employees differs in its format to the Model Fair Processing Notice produced for use for external individuals’ personal data. The Employee Fair Processing Notice is a streamlined version which takes the form of numbered paragraphs.

You will also need to consider what employee information is held (including prospective employee information – e.g. how long do you currently retain prospective job applications?). Further, you will also need to consider what information you hold on former employees, for how long, and for what purpose you retain that information. Your HR department should consider this in detail when analysing the personal data the department holds, and should complete the Personal Data Map (see Appendix 4) in this respect.

You will require to consider your procedures in relation to employee personal data and at what stage to hand out the notice to employees. It is also recommended that current employees are provided with a copy of this notice when finalised.

A separate FPN should be provided to governing body members.

**4.2 Contracts of Employment**

You may require to review and update your model Contract of Employment in relation to data protection. The draft wording provided (see Appendix 6) is self-explanatory and seeks confirmation from the employee that they have read the policy and Fair Processing Notice.

It is recommended that a copy of the Fair Processing Notice should be annexed to the Contract of Employment as well as a copy being given separately to the employee. There is no requirement for an individual to sign this documentation, nor is there a requirement for you to ensure that the Fair Processing Notice is read by individuals it is given to.

**5. Data Sharing**

You will share data – including personal data – with a large number of third-party individuals/organisations for a variety of reasons.

When carrying out your audit of the personal data you hold (see template at Appendix 4) you should consider with whom the personal data is shared, and for what purpose(s).

There are a number of third-party organisations that will likely have access to personal data processed by you. These would include external payroll service providers, Allpay, pension service providers, maintenance contractors, and other contractors.

**5.1 Data Sharing with Data Processors**

The GDPR imposes a requirement on Data Controllers and Data Processors that means both should review the terms of their contractual relationship with each other to bring those existing relationships in line with the terms of the GDPR.

You will therefore require to review your contracts with these third-party data processors and ensure that they are compliant with the requirements of the GDPR. To achieve that, you should not vary the terms of that contract, but rather use an addendum, supplementary to the contract itself, to set out GDPR related matters. This Data Protection Addendum will supplement the pre-existing contractual terms in place.

The Model Data Protection Addendum (Appendix 7) will require to be adjusted to reflect the exact contractual relationship between you and each of your third party processors, and will therefore require to be adjusted in relation to each of your processors.

You will also need to consider the individual clauses within the model as to whether they are suitable as drafted for your relationship with each Data Processor. The Addendum should:

* ensure protection of data subject rights
* provide greater details re the processing itself
* state that personal data may only be processed under documented instruction from the data controller
* confirm the requirements of the processor to notify controller when required to process data due to a legal requirement
* confirm processor staff confidentiality obligations
* confirm arrangements for the processor’s deletion or return personal data at the end of the service provision.

The Schedule to the Data Protection Addendum will require to be updated and revised for each Data Processor Addendum to reflect the personal data processed by the Data Processor.

**5.2 Data Sharing with Data Controllers**

There will be situations in which both you and another organisation process personal data as Data Controllers, and require to share data for such purposes. An example would be a pension service provider who requires personal data to administer the pension service for employees.

When sharing data with another Data Controller, you should enter into a written agreement with them to ensure, as far as practicable, that processing is compliant under the GDPR. An Addendum alone would not be sufficient in these circumstances.

The Model Data Sharing Agreement (see Appendix 8) has been produced for use when you share data with other Data Controllers. The Data Sharing Agreement requires to be entered into with each Data Controller to ensure that each party is complying with the terms of the GDPR in processing personal data. The model Data Sharing Agreement will require revision to reflect the contractual arrangements between each Data Controller party to that agreement.

The ICO is yet to finalise its Data Sharing Code of Practice which will apply to data sharing between Data Controllers. However, a draft Code has been published for consultation and it advises that Data Sharing Agreements are reviewed on a regular basis.[[9]](#footnote-10)

You will need to review the provisions of this model agreement, particularly in relation to security measures. You will also need to populate Part 1 of the Schedule with details of the personal data being shared.

**6. Next steps**

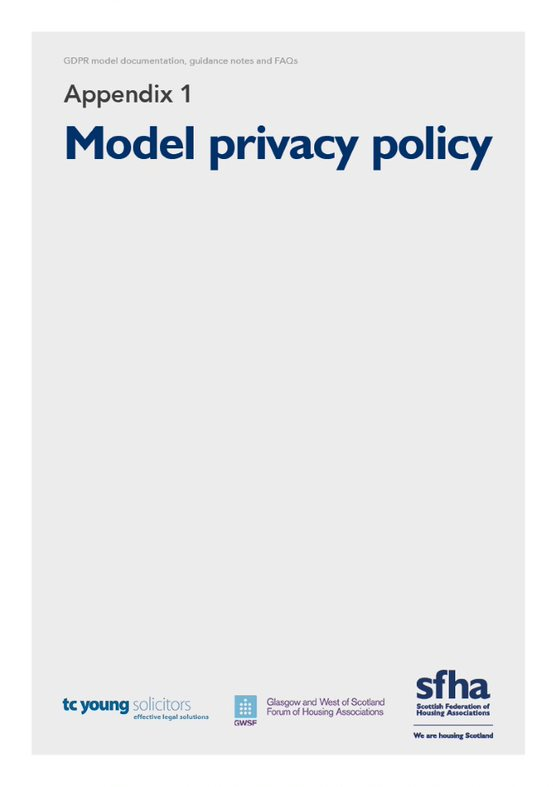
Whilst every effort has been made to produce a suite of documents that will ease the transition from existing policies and procedures to updated polices and procedures (as well as additional documentation), every RSL’s operational functions and practices will differ. It is therefore impracticable to provide a “one size fits all” suite of documents for you to adopt. You will require to adapt these model documents to suit your practices and procedures and the activities which you carry out within your organisation.

You should audit the personal data held by your organisation in accordance with the above notes and Personal Data Map (Appendix 4) in order that the terms of the FPN can be reviewed. If making any changes, you should also contact your Data Processors and other Data Controllers with whom you share information to discuss arrangements for updating your contractual relationships with them.

Additionally, you should also review your policies and procedures to ensure they are in line with GDPR requirements. The following is a non-exhaustive list of policies/procedures that you may have in place currently that you may wish to review:

* Allocations;
* ASB;
* Arrears/Debt recovery
* Membership/Board Members policies
* Policies re security measures
* Staff Handbook and other employment related documents
* Succession/Assignation/Mutual Exchange/Sub-Letting

**Please note that the model documents do not form finalised documentation for immediate use by you, and it is strongly recommended that you take your own independent legal advice when finalising the terms of your documentation.**



**#** [name of RSL]

**PRIVACY POLICY**

**Contents**

1. Introduction p1
2. Legislation p1-2
3. Data p2
4. Processing of Personal Data p3-5
5. Data Sharing p5-6
6. Data Storage and Security p7
7. Breaches p7-8
8. Data Protection Officer p8-9
9. Data Subject Rights p9-11
10. Privacy Impact Assessments p12
11. Archiving, Retention and Destruction of Data p12
12. List of Appendices p13
13. **Introduction**

#[insert RSL name] (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.

1. **Legislation**

It is a legal requirement that 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:**

1. the UK General Data Protection Regulation (“the GDPR”);
2. the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as may be amended by the proposed Regulation on Privacy and Electronic Communications);
3. the Data Protection Act 2018 (“the 2018 Act”) and
4. any legislation that, in respect of the United Kingdom, replaces, or enacts into United Kingdom domestic law, the UK General Data Protection Regulation, 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.
5. **Data**

3.1 The Association holds a variety of Data relating to individuals, including customers and employees (also referred to as Data Subjects). Data which can identify Data Subjects 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”.

1. **Processing of Personal Data**
   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; or
* 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.

**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 prospective Employees at application stage.

4.3.2 A copy of any employee’s Personal Data held by the Association is available upon request by that employee from the Association’s Data Protection Officer (see part 8).

**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). Where consent is being relied on, Data Subjects are free to withhold their consent or withdraw it at any future time.

**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 rely on an additional ground for processing in accordance with one of the special category grounds. These include, but are not restricted to, the following

* 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, social security, or social protection law;
* Processing is necessary for health or social care
* 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 under law

All the grounds for processing sensitive personal data are set out in the GDPR and expanded on in the Data Protection Act 2018.

1. **Data Sharing**
   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 may 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. This will only apply in situations where the third party is a joint controller.
   2. **Data Sharing**

5.2.1 Personal Data is from time-to-time shared amongst the Association and third parties who require to process the same Personal Data as the Association. Whilst the Association and third parties may jointly determine the purposes and means of processing, 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.

* 1. **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).

* + 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.
    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.
    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.

1. **Data Storage and Security**

All Personal Data held by the Association must be stored securely, whether electronically or in hard copy 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 ensure that no Personal Data is left in a place 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 secure 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 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.

1. **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 it becomes known the breach or potential breach has occurred, and in any event no later than six (6) hours after it has occurred, the Association’s 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 whichever means available;
* The DPO must consider whether the breach is one which requires to be reported to the ICO and to the Data Subjects affected and, if appropriate, will 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.

1. **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 appointed a Data Protection Officer (DPO). The Association’s DPO’s 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.

1. **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 request erasure of their Personal Data, 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. Such rights are subject to qualification and are not absolute.

9.3 **Subject Access Requests**

Data Subjects are permitted to view their Personal 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 from the day after 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 or that Personal Data sought to the Data Subject as soon as practicably possible, and in any event, not later than one month from the day after the date on which the request was made.

9.4 **The Right to Erasure**

9.4.1 A Data Subject can exercise their right to erasure (otherwise known as the right to be forgotten) by submitting a request 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.

9.4.3 Requests for Erasure will be considered and responded to by the Association by one month from the day after the date we receive 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.

**9.6 The Right to Rectification**

9.6.1 A Data Subject may request the Association to have inaccurate Personal Data rectified. If appropriate, a Data Subject may also request the Association to have incomplete Personal Data completed.

9.6.2 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 9.6 and will respond in writing to the request.

1. **Privacy Impact Assessments (“PIAs”)**
   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.
   2. The Association shall:
      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
      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 or mitigated. The 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.

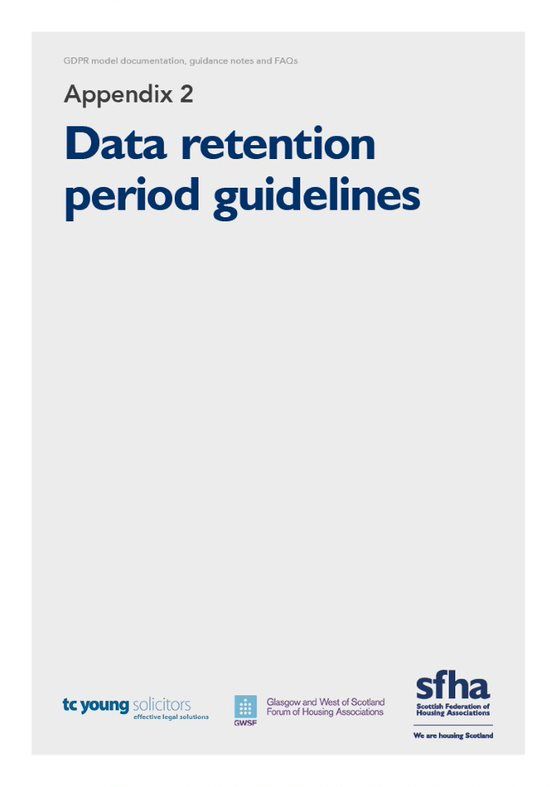
1. **Archiving, Retention and Destruction of Data**

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**

**[*Drafting Note: Appendices to be appended to individual member’s finalised Policy]***

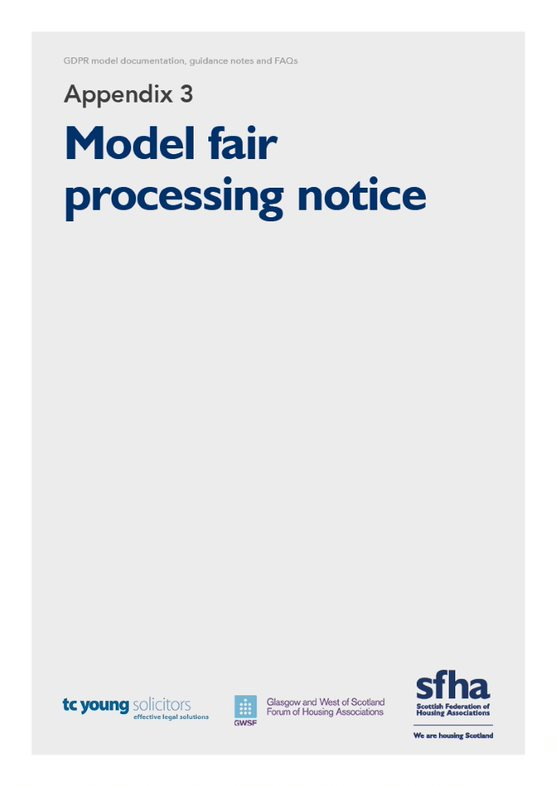
* + - 1. Related Policies
      2. Fair Processing Notice
      3. Model Data Sharing Agreement
      4. Model Data Processor Addendum
      5. Table of Duration of Retention of certain Data



**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 | 5 years after last contact |
| Personal files including training records and notes of disciplinary and grievance hearings | 5 years to cover the time limit for bringing any civil legal action, including 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. |
| Payroll | 3 years after the end of the tax year they relate to |
| Income tax, NI returns, correspondence with tax office | At least 3 years after the end of the tax year they relate to |
| Retirement benefits schemes – notifiable events, e.g. relating to incapacity | 6 years from end of the scheme year in which the event took place |
| Pensioners records | 12 years after the benefit ceases |
| Statutory maternity/paternity and adoption pay records, calculations, certificates (MAT 1Bs) or other medical evidence | 3 years after the end of the tax year to which they relate |
| Parental Leave | 18 years |
| Statutory Sick Pay records, calculations, certificates, self-certificates | 3 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 | 3 years after the date of the last entry |
| 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 | 5 years after cessation of membership |
| Documents relation to successful tenders | 5 years after end of contract |
| Documents relating to unsuccessful form of tender | 5 years after notification |
| Applicants for accommodation | 5 years |
| Housing Benefits Notifications | Duration of Tenancy |
| Tenancy files | Duration of Tenancy |
| Former tenants’ files (key info) | 5 years |
| 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 (e.g. Agendas, notice of meetings etc) | 2 years (this does not refer to minutes of meetings as these must be permanently retained) |
| Minute of factoring meetings | Duration of appointment |



**#[ insert RSL name ]**

**GDPR Fair Processing Notice**

**(How we use your personal information)**

***Drafting Note:***

* ***This document is intended to provide notice to individuals about the use of their personal data. It is important that individuals are informed in clear language of how their personal data will be used - this document must be provided to individuals before any use is made of their personal data.***
* ***Drafting notes have been included at the start of each section explaining the requirements of each section. These drafting notes should be deleted once the Fair Processing Notice (“FPN”) is finalised, and prior to the distribution of the FPN to individuals. We have also provided indicative wording in most sections, however, each section should be reviewed and updated (in plain English) by the relevant data controller to ensure that individuals are appropriately notified. The wording in square brackets may in some cases also be relevant.***
* ***If any decisions or processes are based on automated decision-making (including profiling) then details of this should be included within this notice including the consequences of such processing for the individual.***
* ***This document will require to be adapted by the individual RSL members to suit their practices and procedures and work undertaken. It is designed as a model only with guidance/ drafting notes detailed throughout for ease of finalising the precise terms of the member’s FPN. It is recommended that each member seek their own legal advice when finalising the terms of their Fair Processing Notice.***

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?**

#[**insert RSL name**], ###, a Scottish Charity (Scottish Charity Number  ###), a registered society under the Co-operative and Community Benefit Societies Act 2014 with Registered Number ### and having their Registered Office at ### (“**we**” or “**us**”) take the issue of security and data protection very seriously and strictly adhere to guidelines published in the UK GDPR and Data Protection Act of 2018 (the 2018 Act), together with any domestic laws subsequently enacted.

We are registered as a Data Controller with the Office of the Information Commissioner (ICO) under registration number #**[insert Data Controller number]** and we are the data controller of any personal data that you provide to us.

Our Data Protection Officer is #**[insert name and contact details]**.

Any questions relating to this notice and our privacy practices should be sent to #[**insert contact details**]. ***Drafting Note: Corporate Services/ Housing Team or DPO. RSL to determine***

**How we collect information from you and what information we collect**

***Drafting Note: This section should set out details of: (i) how information is collected (e.g. via website, from third parties, from information provided by the individual etc.); (ii) the personal information collected from the individuals; and (iii) the reasons for collecting this information. This should specify whether this is collected by the data controller directly or received from third parties (where possible details of the third parties should be included).***

We collect information about you to enable us to perform our contractual obligations. You, in turn, are under a contractual obligation to provide the data requested from you to enable performance of the contract (i.e. the tenancy agreement you are party to):

* 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; ***Drafting Note: Individual members must consider how their website is used by data subjects and whether any information is collected from website usage***
* 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);

Under the terms of the tenancy agreement, you are under a required to provide us with the following information:

* name;
* address;
* telephone number;
* e-mail address;
* National Insurance Number;
* Next of Kin;
* #[***insert further personal data you collect from the individual***]

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

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

***Drafting Note: This section should set out the reasons for requiring the information and the legal basis for the processing (for example, if the processing is necessary to carry out a contract with the individual). It should also clearly detail how you will use the personal information. The current list is a suggestion based on some common uses of data and should be adjusted to reflect how the personal data is used in practice.***

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. This includes:

* 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**

***Drafting Note: This section sets out details of when and how any personal data will be shared with third parties. It is important that data subjects are aware of the circumstances where their personal data may be shared and this section should be comprehensive.***

The information you provide to us will be treated by us as confidential /[and will be processed only by our employees within the UK]\* ***Drafting note: Members need to check that whether data is processed (particularly by IT support providers and other online facilities)- see section below***. 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 the Local Authority);
* If we are investigating payments made or otherwise, your information may be disclosed to payment processors, Local Authority and the Department for 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
* **[insert details of any further data sharing arrangements/ third parties who process personal data on behalf of RSL member.] NOTE: I would be keen to discuss further with those in the working group.**

Unless we have a lawful basis for disclosure, we will not otherwise share, sell or distribute any of the information you provide to us without your consent.

**Transfers outside the UK**

***Drafting Note: If personal data will be transferred outside the UK it is important that data subjects are aware of this. Following Brexit, you should now include details of transfers outside the UK specifically. If personal data is stored in the cloud the location of the servers should be confirmed and if outside the UK this should be stated in this notice. This is something that individual member organisations will need to check.***

#[Your information will only be stored within the UK / [We may transfer your information outside the UK] *(\*delete as appropriate)*:

**#[insert situations where personal data is transferred outside UK]** *(\*delete if not applicable)*

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

**#[Insert basis for transfer and relevant safeguards (e.g. decision by the ICO that the third country has adequate safeguards/ details of appropriate security provisions in place.)]**

**Security**

***Drafting Note: It is important that personal information is stored securely and appropriate technical measures are taken to protect this information. This section should set out details of the security measures in place.***

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

#**[insert further details of security processes] *Drafting Note: the individual member organisation will require to confirm their own security measures that are in place and will require to update their FPN with these details. Alternatively, you could provide a link to the organisation’s Data Protection/ Privacy Policy.***

**How long we will keep your information**

***Drafting Note: It is important that personal data is not stored for any longer than it is reasonably required. Data subjects should be notified of how long personal data is stored for, or if this is not possible, then details of the criteria used to determine how long personal data will be kept for. The wording below provides some generic wording, however, this should be updated/specific for each type/use of personal data.***

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:

* **NOTE: TC Young will produce draft retention periods separately which can be adopted or altered. The individual member organisation must be able to demonstrate the requirement to retain the personal data for the specified period.**

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

Our full retention schedule is available at #**[insert where data subject can source retention schedule (e.g. website or in our office)].**

**Your Rights**

***Drafting Note: Data Subjects must be told of their rights in relation to the personal data you hold.***

You have the right at any time to:

* ask for a copy of the information about you held by us in our records;
* ask us to correct any inaccuracies of fact in your information;
* request that we restrict your data processing
* data portability
* Rights related to automated decision making including profiling
* 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 **#[insert DPO contact details/ e-mail address]. You should note that your rights under the UK GDPR and 2018 Act are not absolute and are subject to qualification.**

If you have any complaints about the way your data is processed or handled by us, please contact #[insert DPO details and email address]

If you remain unsatisfied after your complaint has been processed by us, 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:

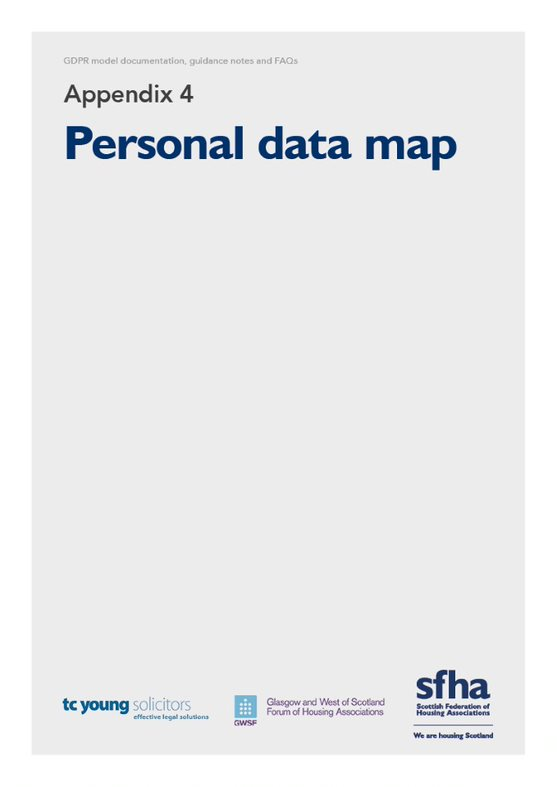
The Information Commissioner’s Office – Scotland

45 Melville Street, Edinburgh, EH3 7HL

Telephone: 0303 123 1115

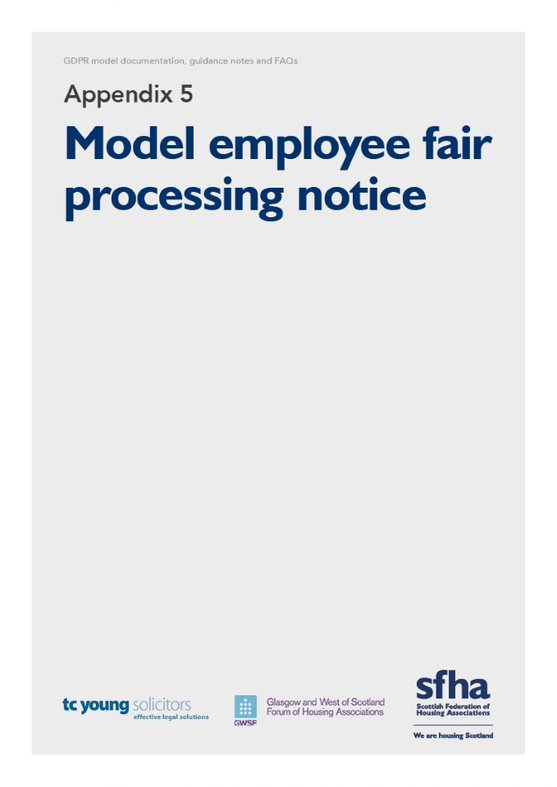
Email: [Scotland@ico.org.uk](mailto:Scotland@ico.org.uk)

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.



**PERSONAL DATA MAP**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Categorise the personal data held.** | **Identify types of personal data held, and in particular, identify sensitive personal data (e.g. medical records, trade union membership)** | **Where did the data come from?** | **In which territory is the data stored AND in which territories is the data used?** | **Why is the data used?** | **Do third parties have access or use to the data, e.g. clients or service providers?** | **On what terms was the data acquired?** |
| *Employee HR files* | *Name, address, payroll details, medical records* | *From employee or generated by organisation* | *This could be different, e.g. data stored in the States but accessed and used across the group.* | *Please provide wide answers, e.g. for day to day administrative purposes.* | *E.g. data processors, payroll providers* | *This will depend on how the data was acquired. E.g. it could be under the scope of an employment contract or it could be via a service agreement. Please consider* ***privacy policies*** *and* ***fair processing notices****.* |
| *Contractors* |  |  |  |  |  |  |
| *Ex-Employee / Alumni* |  |  |  |  |  |  |
| *Customers* |  |  |  |  |  |  |
| *On-Site Vendors* |  |  |  |  |  |  |



**#[ insert RSL name ]**

**Fair Processing Notice**

(How we use employee information)

***Drafting Note:***

* ***This document is intended to provide notice to employees about the use of their personal data. It is important that employees are informed in clear language of how their personal data will be used - this document must be provided to employees (or prospective employees) before any use is made of their personal data.***
* ***Drafting notes have been included at the start of each section explaining the requirements of each section. These drafting notes should be deleted once the FPN is finalised and prior to distribution to individual employees. We have also provided indicative wording in most sections, however, each section should be reviewed and updated (in plain English) by the relevant data controller to ensure that individuals are appropriately notified. The wording in square brackets may in some cases also be relevant.***
* ***If any decisions or processes are based on automated decision-making (including profiling) then details of this should be included within this notice including the consequences of such processing for the individual.***
* ***This document will require to be adapted by the individual RSL members to suit their practices and procedures and work undertaken. It is designed as a model only with guidance/ drafting notes detailed throughout for ease of finalising the precise terms of the member’s Fair Processing Notice. It is recommended that each member seek their own legal advice when finalising the terms of their Fair Processing Notice.***

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. # [**insert name of RSL**] (“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 UK GDPR and Data Protection Act of 2018 (the 2018 Act), together with any domestic laws subsequently enacted. We collect and use personal data for a variety of reasons.

We are registered as a Data Controller with the Office of the Information Commissioner (ICO) under registration number #**[insert Data Controller number]** and we are the data controller of any personal data that you provide to us.

Our Data Protection Officer is #**[insert name and contact details]**.

Any questions relating to this notice and our privacy practices should be sent to #[**insert DPO contact details**].

***Drafting Note: The following paragraph should set out details of: (i) how information is collected (e.g. from third parties, from information provided by the individual etc.); (ii) the personal information collected from the individuals; and (iii) the reasons for collecting this information. This should specify whether this is collected by the data controller directly or received from third parties (where possible details of the third parties should be included). Consider what sensitive Personal Data you hold about employees and on what basis you are processing this. If processing without consent, you must have an alternative basis and must disclose the sensitive personal data processing without consent in this Notice.***

1. We collect the following information from you through a variety of resources (i) directly from you; or (ii) third parties (including employment agencies, pensions services):
2. Name
3. Date of Birth
4. Address
5. Telephone Number
6. E-mail address
7. NI number
8. Personal characteristics such as gender and ethnic group
9. Qualifications
10. Absence information
11. # [***Drafting Note: insert any further personal data collected from employees***]

***Drafting Note: The following paragraph should set out the reasons for requiring the information and the legal basis for the processing (for example, if the processing is necessary to carry out a contract with the individual). It should also clearly detail how you will use the personal information. The current list is a suggestion based on some common uses of data and should be adjusted to reflect how the personal data is used in practice.***

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

* 1. Administration of contracts of employment
  2. Payment of salaries
  3. Recruitment and selection
  4. Pensions and associated benefits, appraisal, training and development
  5. Membership of professional bodies
  6. # [insert any further reasons for processing employee personal data]

***Drafting Note: The following paragraph sets out details of when and how any personal data will be shared with third parties. It is important that data subjects are aware of the circumstances where their personal data may be shared and this section should be comprehensive.***

1. 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 # [***insert frequency, i.e. weekly/ fortnightly***] salary payments;
* To allow your pension provider to process pensions information and handle your pension; (delete if not applicable)
* To allow your electronic payslips to be produced and issued to you (delete if not applicable)
* 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.

***Drafting Note: If personal data will be transferred outside the EEA it is important that data subjects are aware of this. Following Brexit you should nowinclude details of transfers outside the UK specifically. If personal data is stored in the cloud the location of the servers should be confirmed and if outside the UK/EEA this should be stated in this notice. This is something that individual member organisations will need to check.***

1. #[Your information will only be stored within the UK]/ [We may transfer your information outside the UK] *(\*delete as appropriate)*:

**#[insert situations where personal data is transferred outside UK]** *(\*delete if not applicable)*

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

**#[Insert basis for transfer and relevant safeguards (eg. decision by the Commission that the third country has adequate safeguards/ details of appropriate security provisions in place.)]**

***Drafting Note: It is important that personal information is stored securely and appropriate technical measures are taken to protect this information. This paragraph should set out details of the security measures in place.***

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

#**[insert further details of security processes] *Drafting Note: the individual member organisation will require to confirm their own security measures that are in place in relation to employee personal data and will require to update their FPN with these details. Alternatively, you could provide a link to the organisation’s Data Protection/ Privacy Policy.***

***Drafting Note: It is important that personal data is not stored for any longer than it is reasonably required. Data subjects should be notified of how long personal data is stored for, or if this is not possible, then details of the criteria used to determine how long personal data will be kept for. The wording below provides some generic wording, however, this should be updated/specific for each type/use of personal data.***

1. 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 Privacy policy within the staff handbook.

***Drafting Note: Data Subjects must be told of their rights in relation to the personal data you hold.***

1. You have the right at any time to:

* ask for a copy of the information about you held by us in our records;
* ask us to correct any inaccuracies of fact in your information;
* request that we restrict your data processing
* data portability
* Rights related to automated decision-making including profiling
* make a request to us to delete what personal data of your we hold; and
* object to receiving any marketing communications from us.

These rights are qualified and are not absolute.

1. 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: # [ ***insert DPO contact details*** ].

If you have any complaints about the way your data is processed or handled by us, please contact **#[insert DPO details and email address]**

If you remain unsatisfied after your complaint has been processed by us, 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: 0303 123 1115

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 personal and contact details.



**Employment Contract – Data Protection Wording**

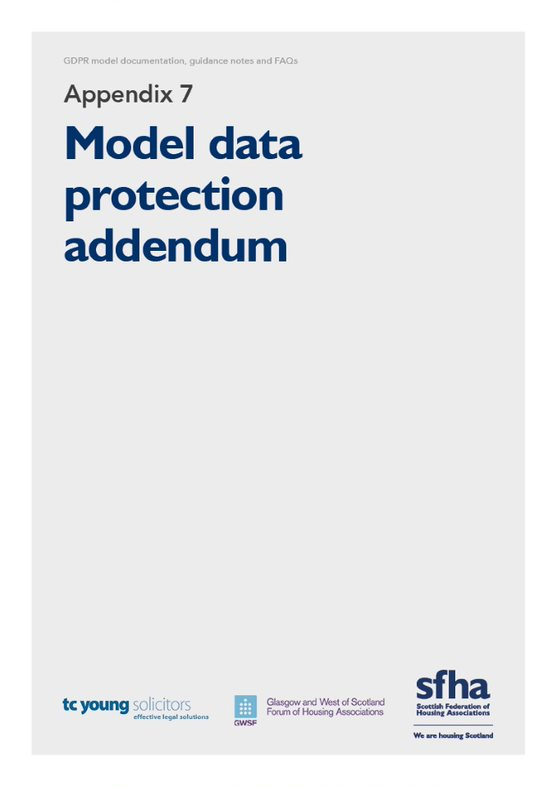
***Drafting Note: Each member organisation will require to adjust the terms of the wording below to fit with the wording of their style Contract of Employment (i.e. the use of “we” may need to be changed to “# Housing Association” or “The Association”)***

***The Employee Fair Processing Notice must be made available to employees/ prospective employees at the outset of processing personal data. To achieve this HR staff my elect to append one copy of the Employee Fair Processing Notice to the Terms and Conditions/ Contract and provide the employee with a duplicate copy, or to any application made available to prospective employees.***

***Members should seek their own independent legal advice in relation to any requirement to obtain consent for processing any sensitive personal data not covered in their Employee Fair Processing Notice. Individual forms of consent that are specific and unambiguous will require to be freely signed by the employee whose additional sensitive personal data you wish to store.***

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 the UK GDPR and 2018 Act. The Fair Processing Notice annexed to these Terms & Conditions/this Contract*(\*delete as appropriate*) (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 Privacy/ Data Protection Policy contains further details regarding Data Protection matters, and the handling of personal data. By signing these Terms & Conditions/this Contract*(\*delete as appropriate*) you confirm that you have read and understood our Privacy/Data Protection Policy*(\*delete as appropriate*) 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 if appropriate.



***[Drafting Note: It is anticipated that specific standard clauses will require to be included within finalised DP Addendums depending on the third party processor and nature of the member’s relationship with them, in which case this draft will require to be updated to reflect that]***

**DATA PROTECTION ADDENDUM**

between

**#[insert name of RSL]**, a Scottish Charity (Scottish Charity Number  #), a registered society under the Co-operative and Community Benefit Societies Act 2014 with Registered Number # and having their Registered Office at # (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**

***[Drafting Note: Further detail will require to be inserted here to confirm relationship between Parties to the Agreement. This will depend on the precise nature of relationship so will require to be adapted for every individual use of this model Agreement.]***

1. The Association and the Processor have entered in to an agreement/ contract to #[insert detail] (hereinafter the “Principal Agreement”/”Principal Contract”);
2. This Data Protection Addendum forms part of the Principal Agreement/Principal Contract (\*delete as appropriate); and
3. 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.
4. **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. **"Applicable Laws"** means (a) Data Protection Act 2018 (DPA 2018), (b) the UK General Data Protection Regulation (“GDPR”); and (c) 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;
    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;
    3. "**Contracted Processor**" means Processor or a Sub-processor;
    4. "**Data Protection Laws**" means UK Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;
    5. "**EEA**" means the European Economic Area;
    6. "**GDPR**" means UK General Data Protection Regulation;
    7. "**Restricted** **Transfer**" means:
       1. *a transfer of Association Personal Data from the Association to a Contracted Processor; or*
       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. "**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;
    2. "**Subprocessor**" means any person (including any third party 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. The terms, "**Commission", "Controller", "Data Subject", "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.
  2. The word "include" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly**.**

1. **Processing of Association Personal Data**
   1. The Processor shall:
      1. comply with all applicable Data Protection Laws in the Processing of Association Personal Data; and
      2. not Process Association Personal Data other than on the Association’s documented **instructions [“of” insert Association staff member details here if appropriate]** 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. The Association
      1. Instructs the Processor (and authorises Processor to instruct each Sub-processor) to:
         1. *Process Association Personal Data; and*
         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

* + 1. 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](file:///C:\Users\awm\AppData\Local\Microsoft\Windows\Temporary%20Internet%20Files\Content.IE5\FGDKD7N7\example_data_protection_addendum.doc#_Ref482951323).
  1. The Schedule to this Addendum sets out certain information regarding the Contracted Processors' Processing of the Association Personal Data as required 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](file:///C:\Users\awm\AppData\Local\Microsoft\Windows\Temporary%20Internet%20Files\Content.IE5\FGDKD7N7\example_data_protection_addendum.doc#_Ref482964294)) confers any right or imposes any obligation on any party to this Addendum.

1. **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.

1. **Security**
   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 the GDPR.
   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.
2. **Subprocessing [*Drafting Note: This clause should be adjusted depending on the arrangements between Parties*]**
   1. The Association authorises the Processor to appoint (and permit each Subprocessor appointed in accordance with this section [5](file:///C:\Users\awm\AppData\Local\Microsoft\Windows\Temporary%20Internet%20Files\Content.IE5\FGDKD7N7\example_data_protection_addendum.doc#_Ref472956474) to appoint) Subprocessors in accordance with this section [5](file:///C:\Users\awm\AppData\Local\Microsoft\Windows\Temporary%20Internet%20Files\Content.IE5\FGDKD7N7\example_data_protection_addendum.doc#_Ref472956474) and any restrictions in the Principal Agreement.
   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](file:///C:\Users\awm\AppData\Local\Microsoft\Windows\Temporary%20Internet%20Files\Content.IE5\FGDKD7N7\example_data_protection_addendum.doc#_Ref478107174).
   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.
   4. With respect to each Subprocessor, the Processor or the relevant shall:
      1. before the Subprocessor first Processes Association Personal Data (or, where relevant, in accordance with section [5.2](file:///C:\Users\awm\AppData\Local\Microsoft\Windows\Temporary%20Internet%20Files\Content.IE5\FGDKD7N7\example_data_protection_addendum.doc#_Ref472933585)), 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;
      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 in the GDPR;
      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

[***Drafting Note: Each member organisation will require to check arrangements with its Data Processors to ascertain where the Processing is taking place – i.e. within UK or outwith. If outwith, where. The Standard Contractual Clauses are not appended to this initial draft for discussion as it is not anticipated that member organisations will be contracting with Data Processors who are Processing Personal Data outwith the UK***]

* + 1. 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.
  1. The Processor shall ensure that each Subprocessor performs the obligations under sections [2.1](file:///C:\Users\awm\AppData\Local\Microsoft\Windows\Temporary%20Internet%20Files\Content.IE5\FGDKD7N7\example_data_protection_addendum.doc#_Ref471379220), 3, 4, [6.1](file:///C:\Users\awm\AppData\Local\Microsoft\Windows\Temporary%20Internet%20Files\Content.IE5\FGDKD7N7\example_data_protection_addendum.doc#_Ref479246263), [7.2](file:///C:\Users\awm\AppData\Local\Microsoft\Windows\Temporary%20Internet%20Files\Content.IE5\FGDKD7N7\example_data_protection_addendum.doc#_Ref482964994), 8 and [10.1](file:///C:\Users\awm\AppData\Local\Microsoft\Windows\Temporary%20Internet%20Files\Content.IE5\FGDKD7N7\example_data_protection_addendum.doc#_Ref482970378), 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.

1. **Data Subject Rights**
   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.
   2. The Processor shall:
      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
      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.
2. **Personal Data Breach**
   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.
   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.
3. **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 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.

1. **Deletion or return of Association Personal Data**
   1. Subject to sections [9.2](file:///C:\Users\awm\AppData\Local\Microsoft\Windows\Temporary%20Internet%20Files\Content.IE5\FGDKD7N7\example_data_protection_addendum.doc#_Ref479850356) and [9.3](file:///C:\Users\awm\AppData\Local\Microsoft\Windows\Temporary%20Internet%20Files\Content.IE5\FGDKD7N7\example_data_protection_addendum.doc#_Ref475523583), the Processor shall promptly and in any event within seven (7) days of the date of cessation of any Services involving the Processing ofAssociation Personal Data (the "Cessation Date"), delete and procure the deletion of all copies of those Company Personal Data.
   2. Subject to section [9.3](file:///C:\Users\awm\AppData\Local\Microsoft\Windows\Temporary%20Internet%20Files\Content.IE5\FGDKD7N7\example_data_protection_addendum.doc#_Ref475523583), 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.
   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.
   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.
2. **Audit rights**
   1. Subject to sections [10.2](file:///C:\Users\awm\AppData\Local\Microsoft\Windows\Temporary%20Internet%20Files\Content.IE5\FGDKD7N7\example_data_protection_addendum.doc#_Ref483162686) 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.
   2. Information and audit rights of the Association only arise under section [10.1](file:///C:\Users\awm\AppData\Local\Microsoft\Windows\Temporary%20Internet%20Files\Content.IE5\FGDKD7N7\example_data_protection_addendum.doc#_Ref482970378) to the extent that the Principal Agreement/Contract does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Laws.
   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](file:///C:\Users\awm\AppData\Local\Microsoft\Windows\Temporary%20Internet%20Files\Content.IE5\FGDKD7N7\example_data_protection_addendum.doc#_Ref482970378) and shall make (and ensure that each of its mandated auditors makes) reasonable endeavours to avoid causing (or, if it cannot avoid, to minimise) anydamage, 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:
      1. to any individual unless they produce reasonable evidence of identity and authority; or
      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
3. **General Terms**

***Governing law and jurisdiction***

* 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
  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***

* 1. 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.
  2. Subject to section [11.2](file:///C:\Users\awm\AppData\Local\Microsoft\Windows\Temporary%20Internet%20Files\Content.IE5\FGDKD7N7\example_data_protection_addendum.doc#_Ref483165090), 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.

***[Drafting Note: see comments above re Restricted Transfers etc and the applicability of standard contractual clauses]***

***Changes in Data Protection Laws, etc.***

* 1. The Association may:
     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
     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***

* 1. 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  before this witness |  | Director/Secretary/Authorised Signatory |
| Print Full Name |  | Witness |
| Address |  |  |
|  |
|  |
| On behalf of the Processoration and the Processein.o customersr  at  on | | |
| by |  |  |
| Print Full Name  before this witness |  | Director/Secretary/Authorised Signatory |
| Print Full Name |  | Witness |
| Address |  |  |
|  |
|  |

**SCHEDULE**

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

Part 1 – Data and Categories of Data Subject

For the purposes of this Data Protection Addendum, the categories of personal or special categories of data being processed are:

Name, Address, Contact Details, Household makeup, language spoken, vulnerabilities or risk factors (including deafness, mental health, physical disability), criminal record, associates **[#amend as necessary]**

The data subjects will be tenants of the Association and members of the tenant’s household.

Part 2 – Nature and purpose of the processing

The Processor will processes Association Personal Data when performing housing management and void management tasks in accordance with the Management Agreement. **[#amend as necessary]**

Parties are processing this data for the following reasons:

the processing is necessary for the performance of the contracts between the Association and its tenants.

**[#add additional grounds as necessary]**

Part 3 – Duration and subject-matter

The subject matter of this Agreement is the execution and performance of the services specified within the Management Agreement, performed by the Processor as Data Processor. **[#amend as necessary]**

The Agreement will remain in place until terminated or until the **[#insert principal contract details]** is terminated, whichever is earlier. **[#amend as necessary]**

Part 4 – Representatives

The Association has an appointed DPO for data protection matters. This contact must be contacted should the Processor;

(a) receive a Data Subject Access request

(b) identify or become aware of a Personal Data Breach.

The Processor requires to provide contact details below of their Data Protection Officer (if applicable) or appropriate contact person in relation to this addendum.

**Contact Details**

Association Contact 1 (#**insert DPO details**)

Name: :

Job Title:

Address:

Email:

Telephone:

Association Contact 2

Name: :

Job Title:

Address:

Email:

Telephone:

Processor Contact 1

Name:

Job Title:

Address:

Email:

Telephone:

Processor Contact 1

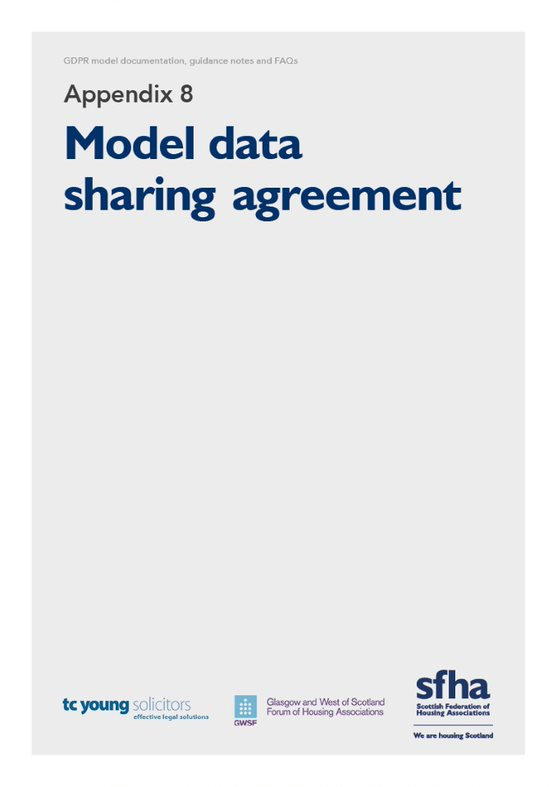
Name:

Job Title:

Address:

Email:

Telephone:



**DATA SHARING AGREEMENT**

between

**#[insert name of RSL]**, a Scottish Charity (Scottish Charity Number  #), a registered society under the Co-operative and Community Benefit Societies Act 2014 with Registered Number # and having their Registered Office at # (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**

***Drafting Note: Further detail will require to be inserted here to confirm relationship between Parties to the Agreement. This will depend on the precise nature of relationship so will require to be adapted for every individual use of this model Agreement.***

1. 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
2. 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.
3. 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. 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:

1. the Data Protection Act 2018;
2. the UK GDPR (“GDPR”); and
3. any legislation that, in respect of the United Kingdom, replaces, or enacts into United Kingdom domestic law, 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 2.3 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 2.4.5.

* 1. In this Agreement unless the context otherwise requires:
     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:

1. the Data Protection Act 1998, in respect of processing undertaken on or before 24 May 2018;
2. the UK General Data Protection Regulation, in respect of processing undertaken on or after 25 May 2018; and
3. 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 UK General Data Protection Regulation, that legislation;
   * 1. 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;
4. **data sharing**

**Purpose and Legal Basis**

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

* 1. 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:
     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 separately and individually responsible for compliance with Data Protection Law;
     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);
     3. it shall comply with its obligations under Part 6 of the Schedule;
     4. it shall not transfer any of the Data outside the United Kingdom except to the extent agreed by the Disclosing Party;
     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:

1. on giving not less than 3 months’ notice in writing to that effect; or
2. 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
   * 1. 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.
   1. 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**

* 1. 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.

1. **BREACH NOTIFICATION**
   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):
      1. the nature of the personal data breach or suspected breach;
      2. the date and time of occurrence;
      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
      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.
   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. 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.
2. **Duration, Review and amendment**
   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.
   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.
   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:
      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
      2. the Information Commissioner or any of his or her authorised staff recommends that the Agreement be reviewed.
   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.
   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:
      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
      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.
   6. Where the Disclosing Party exercises its rights under Clause 4.5, 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.
3. **Liability**
   1. Nothing in this Agreement limits or excludes the liability of either Party for:
      1. death or personal injury resulting from its negligence; or
      2. any damage or liability incurred as a result of fraud by its personnel; or
      3. any other matter to the extent that the exclusion or limitation of liability for that matter is not permitted by law.
   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.
   3. Subject to Clauses 5.1 and 5.2 above:
      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;
      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
      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.
4. **DISPUTE RESolution** 
   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.
   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.
   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 6.2, 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.
   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 8.
   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.
5. **NOTICES**
   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.
6. **Governing law**
   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  before this witness |  | Director/Secretary/Authorised Signatory |
| Print Full Name |  | Witness |
| Address |  |  |
|  |
|  |
| On behalf of #[Party 2]  at  on | | |
| by |  |  |
| Print Full Name  before this witness |  | Director/Secretary/Authorised Signatory |
| 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 it 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
* #[**insert further methods of transport of Data (and delete above if desired)**]

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

* #[**insert details**]

**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**
       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 [**Delete/amend as appropriate]**

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 ***(Drafting Note: though this is no longer recommended so individual members may wish to delete)***

**[Delete/ amend as appropriate]**

* + 1. **Disposal of Assets**
       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.
    2. **Malicious software and viruses**

Each Party must ensure that:

* + - * 1. PCs used in supporting the service are supplied with anti-virus software and anti-virus and security updates are promptly applied.
        2. All files received by one Party from the other are scanned to ensure that no viruses are passed.
        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**

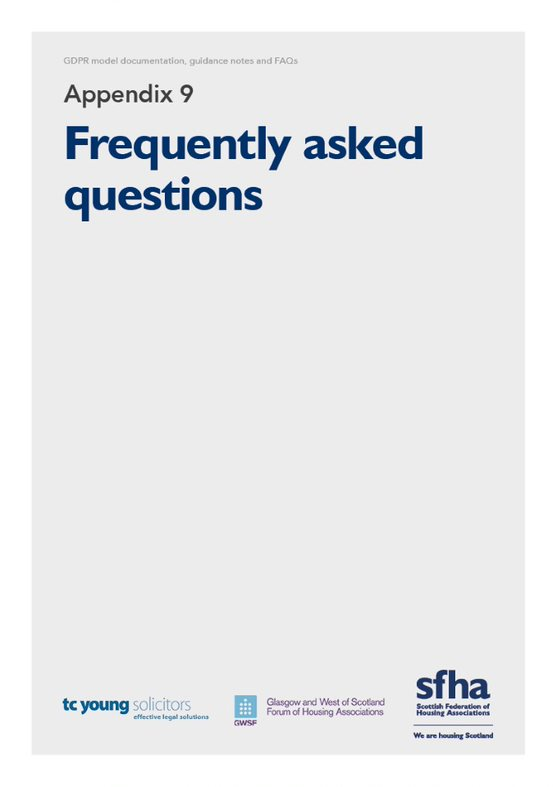
The Disclosing Party shall make reasonable efforts to ensure that Data provided to the Data Recipient is accurate, up-to-date and relevant.

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.



**Contents**

Introduction p1

Document Retention p1-2

Model Fair Processing Notice p2-4

Model Employee Fair Processing Notice p4-5

Consent p5-6

Newsletters p6-7

Photographs p7-8

Data Protection Officers p9-11

Liability p11

Subject Access Requests p12-13

Model Privacy Policy p13

Right to Be Forgotten p14

Data Sharing p14-16

Scottish Housing Regulator p16-17

Online considerations p18

Brexit p18-20

**Frequently Asked Questions**

**Introduction**

This appendix outlines some of the frequently asked questions regarding this guidance by SFHA and GWSF members in relation to this model documentation and GDPR/Data Protection in general.

Broad answers to these questions have been provided by TC Young, but it is important to note that this is intended purely as a steer and is not a substitute for legal advice that will be required to ensure compliance with GDPR requirements. The questions are divided into the following categories:

* Document Retention
* Model Fair Processing Notice
* Model Employee Fair Processing Notice
* Consent
* Newsletters
* Photographs
* Data Protection Officers
* Liability
* Subject Access Requests
* Model Privacy Policy
* Right to Be Forgotten
* Data Sharing
* Scottish Housing Regulator
* Online considerations
* Brexit

**Document Retention**

**Question 1: *What kind of internal document retention schedule should we have in place? Do we have to keep documents in a set format?***

**Answer:** Better to avoid rigid rules and have ‘guidelines’ instead – as a case by case approach is likely to be needed. The guidance provided within the SFHA/GWSF guidance and NHF’s more detailed document retention schedule should be a useful steer.

Under data protection legislation there is no requirement to retain documents in any set format. This means there is no requirement, in terms of data protection, to retain a hard copy if documents are kept electronically. You may however still wish to do so as an additional back up. You should also consider any relevant polices and other legal and/or regulatory requirements where determining if hard copy documents require retention.

**Question 2: *Should we retain data beyond a certain period of time?***

**Answer:** A rule of thumb is that data should not be held five years after the relationship has ended, but it is important to take this on a case by case basis. Some RSLs may feel it is reasonable to dispose of information within a shorter period, where there are no issues (e.g. arrears) with a former tenant.

**Question 3: *What kind of exceptions are there to this rule?***

**Answer:** Solicitors should retain a housing file for 10 years by Law Society guidelines in relation to any matter for which you have sought legal advice.

**Question 4: *How long should we retain governing body minutes?***

**Answer:** Governing body minutes must be retained permanently, but the notices of meetings, agendas etc. of such meetings can safely be destroyed after two years in order to allow publishing of same under FOI legislation.

**Question 5: *The First-tier Tribunal on factoring matters asks for information going back ten years – should we keep information on factored owners for this length of time?***

**Answer:** No. If you do not have the information you cannot provide it. You should only keep this documentation for that period of time if you have a basis for doing so.

**Model Fair Processing Notice**

**Question 6:**  ***Is the Model Fair Processing Notice designed to supplement the tenancy agreement so that access for maintenance, distribution of newsletters and other matters are covered without having to change the Agreement itself?***

**Answer:** Yes. Issuing the FPN means that no changes will need to be made to the tenancy agreement itself.

**Question 7: *When should we issue our Fair Processing Notice to new tenants?***

**Answer:** New tenants should be provided with a copy of your FPN at application stage, or the first point you obtain any personal data- whichever is earlier.

If the data is received from a third party, such as the local authority by way of a section 5 referral, the Notice must be provided when you first communicate with the individual or disclose their data to someone else. In any event, it must be provided no later than one month of obtaining the data.

**Question 8: *What method should we use to issue the FPN to tenants?***

**Answer:** Posting hard copies is better than email. However, if an email address is known, both mediums should be used.

**Question 9: *Which other existing customers should we issue with a Fair Processing Notice?***

**Answer:** Any customers who you hold data for. This will include (for example) housing applicants, factored owners and members of the RSL.

**Question 10: *Could we add a Fair Processing Notice to housing application***

***forms?***

**Answer:** It is okay to add an FPN to the application pack, but you should not have it as an appendix to the form itself. The FPN requires to be a standalone document.

**Question 11: *Could we issue one catch-all FPN to all customers who require it rather than develop separate FPNs for each type of customer?***

**Answer:** You can use one customer FPN template. There is no need to specify a specific FPN for each individual whose data is processed.

**Question 12: *How often should we review our FPN?***

**Answer:** There is no set time period around how often you should review your FPN. However, the ICO advises reviews should be regular and if there is a significant change to your operations, or services that you are providing, you should review your FPN – e.g. if you begin providing a factoring service. We suggest that in light of changes to working practices since the pandemic struck that FPNs are reviewed now, if they have not already been reviewed, to ensure they reflect the current working practices within your organisation.

**Question 13: *Do we need to issue anything to former tenants?***

**Answer:** No. As there is no way to contact in many cases, it would not be practical to issue an FPN. However, a copy of the FPN on the website is deemed sufficient in the circumstances.

**Question 14: *Could we issue a summary FPN with a link to the full copy?***

**Answer:** It is recommended that the whole FPN is issued. However, a summary of this could also be provided as a quick reference guide.

**Question 15: *What about complaints? Do we need to cover this in the FPN – and do we need to issue anything to complainants?***

**Answer:** Yes, you should cover this in two separate areas of the FPN. You should cover this under “How we collect information from you and what information we collect”. You would collect information from a tenant when they make a complaint, and you would receive information from third parties when a third party makes a complaint about a tenant. You do not need to issue an FPN to non-tenant third parties from whom or about whom information is collected, but it is recommended they are at least directed to the online version of your FPN.

**Question 16: *Is it covered off in the FPN that we may hold information on tenants and sharing this with contractors without necessarily the knowledge or consent of the tenant? For example: if we were to flag up violent behaviour/insist two people always attend any visit?***

**Answer:** This should be covered by the FPN so that no consent is required.

**Question 17: *Should the FPN cover CCTV images?***

**Answer:** Yes, the FPN should cover CCTV. CCTV data is usually overwritten so you only have recent days; and if you do not hold the data, it is not governed by the GDPR.

**Model Employee Fair Processing Notice**

**Question 18: *What needs to be issued to staff and job applicants?***

**Answer:** All staff should be issued with an FPN – and the SFHA/GWSF guidance includes a model that can be adapted for this purpose. Recruitment packs should include an FPN for employees; however, you need to ensure that it is not attached to the application form, rather just included in the pack. You can use the same FPN for job applicants as, otherwise, it would be far too onerous to have various FPNs for issuance.

**Question 19: *What about former employees?***

**Answer:** It would not be practical to contact former employees, as you may not have contact details.

**Question 20: *What about governing body members?***

**Answer:** All governing body members must be issued with an FPN.

**Consent**

**Question 21: *We hold information on tenant’s next of kin. Do we need to obtain consent for this information?***

**Answer:** It would not be possible or practical to seek consents under these circumstances and it is not recommended that you do so.

**Question 22: *Sometime MSPs or MPs will contact us on behalf of a tenant. What kind of mandate/consent is required?***

**Answer:** A mandate should be sought from any elected representative (MP, MSP or Councillor) who requests data on behalf of a tenant. If the elected representative or the tenant refuse to provide a mandate, legal advice should be taken - as in most cases you cannot provide the information lawfully without the mandate.

If an RSL is not satisfied by the mandate provided by the elected representative, then they may wish to seek one directly from the tenant.

**Question 23: *We collect National Insurance numbers to help individuals process Universal Credit claims – do we need consent for this?***

**Answer:** In most circumstances, the legitimate interest ground cannot be relied on since RSLs were reclassified as public authorities in November 2019 (for the purposes of FOI). Other bases for processing which might apply are that NI numbers are needed to fulfil contractual obligations (in the tenancy agreement).

**Question 24: *What are the implications of “special categories” in the GDPR?***

**Answer:** Special categories of personal data require more protection due to the sensitive nature of information. In order to process this data, you need to identify an additional legal basis for processing the sensitive data from a separate list. The additional grounds for processing sensitive personal data include: consent, processing is in the public interest, or if there is a life and death situation (to protect the data subject’s vital interests).

**Question 25: *We keep notes on a tenants’ file regarding disabilities – what do we need to consider in terms of consent moving forward?***

**Answer:** Since this would be classed as special category personal data (or sensitive data), you would need to identify one of the usual GDPR grounds for processing and also an additional ground relevant to special category data. If relying on consent, this has to be clear, unbundled, and unambiguous and has to be on an opt-in basis - i.e., the consent form cannot be lumped in with other terms and conditions. You need to ensure that you are holding clear records demonstrating the obtaining of this consent.

**Newsletters**

**Question 26: *Do we need to seek consent from tenants in order to distribute our Newsletter?***

**Answer:** In the majority of cases, the distribution of the Newsletter will not require additional consent and can be covered in the FPN.

**Question 27: *Would advertising Contents Insurance constitute direct***

***marketing?***

**Answer:** No – as this would not be a marketing services provided by RSLs.

**Question 28: *Would promoting the services of our income maximisation officer constitute direct marketing?***

**Answer:** No. This is not a paid for service, and available to tenants as part of their tenancy agreement.

**Question 29: *What about promoting our new developments?***

**Answer:** Promoting the work of the RSL is legitimate and would not constitute direct marketing.

**Question 30: *What about promoting our mid-market rent properties?***

**Answer:** As MMR is provided through a subsidiary, this would not be directly marketing services provided by the RSL. However, even if it were, it is legitimate to promote the work of the RSL such as new developments.

**Question 31: *Is there anything we could include in a Newsletter that would constitute direct marketing?***

**Answer:** Where a newsletter was promoting additional, charged for services by the RSL that are over and above the tenancy agreement. For example – if the RSL offered a charged for furniture service or charged for boiler replacement service.

**Question 32: *What kind of consent would be needed where we did have direct marketing in our Newsletter?***

**Answer:** You would need to seek consent from every tenant if you include direct marketing, so it is advised that this is kept separate from the tenant newsletter if you intend to do so.

**Photographs**

**Question 33: *We have photographs in older documents such as annual reports and newsletters where we did not seek consent – do we need to remove these?***

**Answer:** For any person captured in the pictures, you would require to obtain their consent to continue using their pictures. However, this is not practical and the risks of it being challenged are low. It is best to restrict the seeking of consent in these cases to people clearly identifiable, and to try to avoid sensitive images such as within care homes or of children.

**Question 34: *When taking group photographs of the audience at our AGM, what consent to do we need to get?***

**Answer:** You only require consent of those who are individually identifiable – crowds are not necessarily an issue. For example, you would not be able to identify every person from a picture taken at a football stadium of several thousand people. However, you would be able to identify three people who have their picture taken after winning the raffle prize. In the latter event, you would seek consent for taking pictures of those persons.

**Question 35: *If the deciding factor is whether someone can be individually identified, then the quality of digital images is so good nowadays that pretty much any crowd scene could come under that umbrella, and with face recognition software it is (apparently) quite easy to identify or tag an individual. Does this mean we would have to get consent from everyone attending an AGM/Gala day?***

**Answer:** The position is where someone is individually identifiable in a picture, you need to obtain their consent. However, where there is a large crowd of people, it would be unlikely that you would require to obtain consent of everyone attending an AGM. You have to take this on a case-by-case basis as to how many people are attending the AGM or Gala Day, and as to whether it is practical at the outset to obtain everyone’s consent for taking pictures.

**Question 36: *We have a number of photographs on file but cannot determine if we have sought consent. Can we keep these without seeking consent?***

**Answer:** If you wish to keep these on file, you must reaffirm consent.

**Question 37: *How long should we hold photographs?***

**Answer:** This depends on the wording of your consent form. It is good practice to refresh consent after 2 years. Therefore, you may want to work with that guide of 2 years for how long you use the photographs.

**Question 38: *We have photographs of our staff on our website. We did not seek consent before putting up on website – do we need to?***

**Answer:** Yes. You must seek consent from all staff before using photographs for this purpose.

**Question 39: *How specific does the consent need to be – i.e. can we use a general “Association Newsletters” and “Association Annual Reports” etc., or do they need to be more specific with regard to the actual newsletter or annual report they are going to be used in? Do we need to give a timeframe in which the photograph will be used without refreshing consent?***

**Answer:** You should seek specific consent for use of their photograph – you should detail that the picture will be used on the RSL’s website, newsletter, annual reports and provide an issue date if possible. Consent also requires to be freely given, for a specific purpose, and positively affirmed (i.e. opt in rather than opt out).

**Data Protection Officers**

**Question 40: *Do RSLs need to have a DPO?***

**Answer:** It is mandatory for all RSLs to appoint a DPO. The DPO does not need to be a member of the RSL’s staff. Many mid-sized or smaller RSLs are out-sourcing DPO services or appointing a joint DPO. If the DPO is an internal member of the RSL’s staff, there must not be a conflict of interest with their other duties (so, for example, they cannot be a governing body member). The DPO also cannot be penalised or dismissed for performing their tasks and is not personally liable for any breaches of the GDPR. The DPO should report to the highest level of management.

**Question 41: *The requirements for a DPO state that the role cannot be carried out by the CEO. Could there be any exemptions to this rule – especially in smaller organisations where the CEO might be best placed to carry out the role?***

**Answer:** Unfortunately, there are no exemptions to this rule. The ICO has advised that the DPO can never be the CEO in any circumstances.

**Question 42:** ***Are there any other roles within the organisation that would preclude an individual from being our DPO?***

**Answer:** The DPO can undertake other tasks not associated with data protection for the organisation. However, those tasks cannot conflict with the duties and responsibilities of a DPO; there must not be a conflict of interests. The DPO must undertake their tasks in an independent and impartial manner.

The test for whether there is a conflict of interests or not is whether the DPO holds a position within the organisation that leads him or her to determine **the purposes and the means of the processing of personal data**. If the DPO holds a position where he/she is determining the purposes and means of processing data, then they cannot be a DPO.

For example, someone who is Head of IT would make decisions regarding data collection, storage, and means of processing so they would not be able to be a DPO.

**Question 43:** ***That being the case, when would an internal member of staff be appropriate to appoint as our DPO and at what level should they be in the organisation?***

**Answer:** As above, the test for whether there is a conflict of interests or not is whether the DPO holds a position within the organisation that leads him or her to determine **the purposes and the means of the processing of personal data**. If the DPO holds a position where he/she is determining the purposes and means of processing data, then they cannot be a DPO.

Once in position, the DPO must report directly to the highest level of management and must be given the required independence to perform their tasks.

**Question 44: *Can we share a DPO with another organisation(s)?***

**Answer:** Yes – the ICO advises that: “*GDPR allows for the DPO to have responsibility for more than one organisation, so smaller HAs may wish to negotiate such a joint relationship with other smaller HAs to see if it is feasible for their circumstances. Moreover, the service may be procured externally through, for example, the HAs solicitors.*” It would be crucial that the person appointed as the DPO had a good understanding of that RSL’s working practices etc.

**Question 45: *Has the Information Commissioner produced any guidance on***

***DPOs?***

**Answer:** The ICO guidance on DPOs is available here: [ICO Guidance on DPOs](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/).

**Question 46: *Could someone be a DPO for the HA’s subsidiary, and vice***

***versa?***

**Answer:** The ICO’s position on this is that if someone understands the business but is not involved in the day to day running of the organisation, they may be appointed as a DPO. However, the DPO is expected to a have an expertise or knowledge in data protection matters which is proportionate to the size of the organisation.

**Question 47: *What is the DPO required to do?***

**Answer:** The role of the DPO is to ensure compliance and report breaches of the GDPR. They must also advise and monitor the RSL’s staff and co-operate and consult with the ICO.

**Question 48: *What are the required qualifications and experience of a DPO?***

**Answer:** The ICO has advised currently that the DPO does not have to have any specific, precise credentials, but the experience and skills that the appointed person has should be proportionate to the type of processing that you carry out. The DPO should also have knowledge of the industry and data protection matters in general. Training should be undertaken if required.

**Question 49: *The Fair Processing Notice requires us to name an individual as the DPO – could we make this the job title rather than name an individual? Would this be the case if it was a consultant?***

**Answer:** It would be prudent to name the DPO unless you were recruiting external consultants (who would be more likely to change on a more frequent basis). In the event that the DPO changes (e.g. when s/he leaves their post), it would be good practice to advise tenants of the change in the next newsletter.

**Liability**

**Question 50: *With whom does the liability lie for a breach in data protection and what are the penalties?***

**Answer:** The GDPR now provides for liability for both the Data Controller and the Data Processor. Previously, only the Data Controller was liable in the event of a data protection breach. However, the liability of the breach will depend on the nature and cause of the breach and the data processing agreement in place.

Penalties for a breach can be either up to €20 million or 4% annual global turnover, whichever is higher. Penalties for failure to report a breach can be either up to €10 million or 2% annual global turnover, whichever is higher.

The DPO is not personally liable for data protection compliance.

**Question 51: *If a contractor suffers a breach – who is responsible?***

**Answer:** The controller (i.e. the RSL) can now be held liable for the breach. However, again, liability depends on the nature of the breach. This is why it is important to have a Data Processor Agreement (Model Data Protection Addendum) in place to regulate the position in respect of data protection.

**Subject Access Requests (SARs)**

**Question 52: *The GDPR changes the time frame to respond to one month after receipt – does this meant that we will have a shorter time to respond in certain months (e.g. February)?***

**Answer:** SARs must be complied with as soon as possible but no later than one month from the day after receipt of the request. One month is to be taken as the same day the following month.

For example, a request received on 01 July would need to be complied with by 02 August.

**Question 53: *Should we have in place a set proforma for responding to Subject Access Requests?***

**Answer:** You could have template documentation in place and a policy for responding to Subject Access Requests. However, it must be made clear to the data subject that completion of the form is not mandatory. SARs must be complied with regardless of the method of the request. This includes verbal requests. The data subject does not even need to state that they are making a SAR.

**Question 54: *What happens if someone asks for all data held? Is there any way we can refuse vexatious requests?***

**Answer:** This depends on the specific circumstances, how much information you hold for that person, and whether it is feasible for the RSL to provide the information requested. There is provision for you as the Data Controller to clarify the request as to what specific information they want.

If requests are repeated, excessive, and overlap with each other, you may refuse to comply with it within one month of receipt of the request. Requests are not excessive simply because a large amount of information has been requested. Similarly, you may charge a ‘reasonable fee’ for complying with repeated requests or duplicate copies of data.

**Question 55: *What information should we redact?***

**Answer:** Redactions should be a last resort when providing data which refers to third parties. In the first instance, you should seek, where possible, to obtain the third parties’ consent for disclosure. If consent is not provided, you should consider whether it would nonetheless be reasonable to provide the un-redacted versions. If consent is not given and it would not be reasonable to disclose, you should redact any third- party references and any data that could identify a third-party – for example, the name of a neighbouring complainer. You should also redact legally privileged advice and police requests.

**Question 56: *How should we treat requests for CCTV footage?***

**Answer:** Requests for viewing CCTV footage or copies of same should be treated the same as any other SAR. However, if third parties are captured in the footage, you should obtain their consent prior to disclosure. The process should be the same as when written data is requested. If consent is not given by the third-parties, you should consider whether disclosure would nonetheless be reasonable in the circumstances. If it would not be reasonable, you should attempt to blur the faces of the third-parties.

**Question 57: *What if a solicitor requests data about someone who is not their***

***client?***

**Answer:** If a solicitor requests data about an individual who is not their client, the data should not be supplied unless there is a court order for disclosure or if the data subject agrees. For example, if a solicitor acting for an injured tenant wants to know if the tenant responsible for the injury is insured.

**Model Privacy Policy**

**Question 58: *What level of detail do we need to include in our privacy policy? The model covers a number of aspects that we would prefer to cover in procedures, and we wondered if there was scope for RSLs to separate these out in order to make our policy briefer?***

**Answer:** You could separate the Model Privacy Policy into a Policy document and Procedure document to make each document briefer.

**Question 59: *How widely do we need to publicise our Privacy Policy?***

**Answer:** This must be accessible and it is recommended that this be published on your website.

**Right to Be Forgotten**

**Question 60: *The GDPR contains a new “right to be forgotten” – should we have in place a policy regarding this?***

**Answer:** It is recommended that you do not set down specific rules on how you will deal with this, as you need flexibility in how it is applied on a case by case basis. There are exemptions to the GDPR which may also apply to the ‘right to be forgotten’, such as where the information is required for a legal claim. For example, if a former tenant tries to exercise their right to be forgotten but has an outstanding arrears balance which you are intending to pursue, the request may not need to be complied with.

**Data Sharing**

**Question 61: *We share data with large companies -– e.g. Allpay, HMRC and the Pensions Trust – do we need to put in place a Data Sharing Agreement?***

**Answer:** It is likely the bigger companies will have their own data sharing agreements, so you may not need the SFHA/GWSF model. You are, however, likely to need legal advice on the one you are asked to sign.

**Question 62: *What do we need to get contractors to sign/issue to contractors? And what if they do not sign?***

**Answer:** You would send contractors the Data Processor Agreement (also referred to as the Model Data Protection Addendum) to sign up to. If they do not sign, you need to make a decision whether you still want to use the contractor. If you choose to still use the contractor, you could provide them with a shortened statement (taken from the Data Processor Agreement) setting out what you expect of them in respect of Data Protection and their compliance with the GDPR.

**Question 63: *What if controllers that you share data with refuse to sign up to the Data Sharing Agreement?***

**Answer:** You need to determine whether the controller is a Joint Controller. There is only an obligation under the GDPR to enter into a Data Sharing Agreement where both parties are deemed “joint controllers”. This is where the two Data Controllers are acting together in deciding the purposes and manner of processing the personal data. The alternative would be two parties working as independent data controllers, acting in common with a common pool of data. A good example of this is the Pensions Trust who are declining to enter into a Data Sharing Agreement as they deem the relationship between them and the HA as being that of two independent Data Controllers, and as such, no Data Sharing Agreement is required.

**Question 64: *When do we use a Data Processing Agreement/Addendum and when do we use a Data Sharing Agreement?***

**Answer:** The Data Processing Addendum is for use between the RSL and any organisation that may process data on the RSL’s behalf. For example, when instructions are sent to a sheriff officer for an eviction to be carried out, the sheriff officer is a data processor.

Data Sharing Agreements should be entered into with other data controllers. These are organisations which hold the data for their own purposes. The example given in the guidance is that of a pension service provider who requires to process RSL employees’ data to administer a pension service.

**Question 65: *Who should we sign a Data Sharing Agreement with?***

**Answer:** Data Sharing Agreements should only be entered into with other data controllers who are in direct contact with the RSL and who process the data for a common purpose. Organisations with this relationship are known as joint controllers. The GDPR states that organisations which jointly determine the purposes and means of processing will be joint controllers. For example, you would **not** need to sign a Data Sharing Agreement with Royal Mail, but you would for a pension services provider.

**Question 66: *Does the Data Protection Addendum require to be signed?***

**Answer:** The Data Protection Addendum does not need to be signed in order to make it legally binding. However, a signed version would enable it to be easily relied on if ever necessary.

**Question 67: *What about Common Housing Registers?***

**Answer:** A Common Housing Register would need to have its own FPN as they are the data controller. This can be printed /scanned and passed on to applicants.

There would ideally be one data-sharing agreement for the partners to sign up to, and a common FPN could be used as long as it listed the DPO or other data protection contacts in each HA.

**Question 68: *Do we need any agreement in place with the police?***

**Answer:** Generally speaking, no. There are exceptions to the GDPR which would apply where Police are carrying out investigations.

**Scottish Housing Regulator**

**Question 69: *Are SHR data processors/data controllers, e.g. because of information that RSLs give them (board members’ details, AGM attendance, notifiable events, membership info if requested)? Likewise, OSCR for senior staff and board info? And funders such as Big Lottery?***

**Answer:** The Scottish Housing Regulator would be a Data Controller, as would OSCR. This is because they both are not processing this information on your behalf, but are determining the means and method for processing the information you share with them.

**Question 70: *Do we require a Data Processing/Data Controller agreement with the SHR?***

**Answer:** The SHR has confirmed that as the Regulator for social landlords, they are not a data processor who processes personal data on behalf of RSLs (or local authorities).  RSLs have a legal obligation under the Housing Act to provide the SHR with the information that is necessary for it to discharge our statutory functions. So a data processor/ controller agreement is not appropriate for the relationship.

**Question 71: *Will there be any additional questions in the Annual Return on the Charter relating to GDPR – and will the SHR play any role in the regulation of GDPR?***

**Answer:** The SHR has confirmed that they do not envisage having any direct role or asking any additional questions in the ARC regarding GDPR.  The SHR even removed a proposed regulatory requirement relating to registration with the ICO in order to submit data to them, as the registration requirements have changed under GDPR and this was no longer necessary.

**Question 72:** ***The SHR’s new regulatory framework requires us to collect data relating to each of the protected characteristics for existing tenants, new tenants, people on waiting lists, governing body members and staff. How can we do so and still remain GDPR compliant?***

**Answer:** The data collected in this regard for this purpose should be completely anonymised in such a way that it is in no way linked to the individual providing it and cannot be used to identify that individual.  The data should also be anonymous at the point of collection and not linked to the tenant’s housing file.  This means it is no longer personal data and therefore no longer covered by the GDPR.

Please note that some protected characteristics – such as age and disability – may be necessary to collect in order to deliver services (e.g. you must be at least 16 years old to be a tenant). In these circumstances, you should assess whether the data is also sensitive personal data or not. If the data is sensitive, then it will likely be necessary to obtain the tenant’s consent before collecting and processing. Legal advice should be taken if the tenant refuses to provide consent, as there will likely be another basis for processing which applies.

In all circumstances, regardless of whether the data is sensitive or not, you will need to ensure you have a basis for processing. In most cases, that will be that the processing of such data is necessary under the contract (for example, collecting the tenant’s age).

Any data in relation to protected characteristics or which is sensitive personal data must be securely stored and not be shared with third parties without the Data Subject’s consent or until legal advice is taken.   In terms of the new regulatory requirement, this data should only be collated or shared on an anonymised basis – which means it is no longer personal data and is not subject to the GDPR.

More guidance on how to collect this data relating to protected characteristics on a truly anonymous basis will be provided as part of the SFHA Self-Assurance Toolkit in 2020.    The SHR will begin to assess RSL compliance against this requirement in April 2021.

**Online Considerations**

**Question 73: *Are there any particular GDPR implications for HAs which give tenants (and relevant staff) access to tenants’ online accounts?***

**Answer:** No, as long as systems are secure.

**Question 74: *We have automated systems in our e-mail system that will produce an out of office message when a staff member is off ill – are there any issues around this?***

**Answer**: There may be GDPR implications for where there are procedures such as an automated absence management system which tells staff someone is off ill, as this is sharing personal data and possibly sensitive personal data.

**Question 75: *Do emails require to be encrypted?***

**Answer:** There is no blanket obligation to use secure/encrypted emails in any situation. The GDPR does, however, require organisations to put into place appropriate technical and security measures to ensure the secure transfer of data and it specifically suggests email encryption as a method for doing so. Therefore, using encryption or password protected emails for special category data would certainly be a sensible course of action in order to limit the risks of sensitive data being unlawfully processed or disclosed.

Whilst not mandatory per se, the GDPR does require steps and measures and this would be one of them. It would, therefore, be sensible to use encryption when storing any electronic data and password protecting any sensitive data in particular.

**Brexit**

**Question 76: *Is the GDPR still force following Brexit?***

**Answer:** From 1 January 2021, the EU GDPR was replaced by the new UK GDPR. The UK GDPR applies to the processing of personal data where a business is located in the UK or offers goods/services to the UK. The reality is that the UK GDPR largely mimics its EU counterpart, and you are not likely to notice any material differences in day-to-day compliance.

**Question 77: *How will Brexit impact on the Data Protection arrangements within my organisation?***

**Answer:** Brexit will have a minimal impact on your organisation’s Data Protection arrangements unless your RSL currently transfers data to the EU/EEA. The most likely example of where this might be an issue is if the organisation’s storage cloud is held in an EU/EEQ territory.

**Question 78: *Does this mean we don’t need to anything following Brexit unless our storage cloud is held in an EU/EEQ territory?***

**Answer:** Whilst this is the most likely circumstance to require action, all organisations should take time to review the data mapping exercise undertaken prior to the GDPR being implemented. It is important to revisit where data comes from and where you send it to. Once that has been revisited, organisations need to consider how that data is shared If it is shared with an organisation within the EEA.

It is also advisable to revisit the terms of your Privacy or Fair Processing Notices that have been prepared and update those as necessary.

You may also wish to consider the organisation you share data with as your data processors and review the contractual arrangements in place with them, as those contracts may require to be updated in light of Brexit depending on how/where they store data.

The practical impact is not likely to be significant, but you should consider undertaking a review as set out above of (i) your data mapping, ensuring it remains up to date; (ii) privacy or fair processing notices and (iii) relationships with third parties, particularly your processors.

**Question 79: *Can we still transfer data to and from the EU/EEA?***

**Answer:** Yes. The EU-UK Trade and Cooperation Agreement stipulated that for a period of up to six months from 1 January 2021, there would be no changes to the way businesses send personal data from the EEA to the UK. After such time, personal data transfers from the EEA to the UK must be subject to additional safeguards unless an adequacy decision is obtained. Such an [adequacy decision was reached on 28 June 2021](https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/06/ico-statement-in-response-to-the-eu-commission-s-announcement-on-the-approval-of-the-uk-s-adequacy/) and allows for the free flow of data between the UK and EU/EEA except in relation to certain immigration data.

**Question 80: *What is an adequacy decision?***

**Answer:** The European Commission can deem any country in the world as operating at an “adequate” level. The adequacy decision in respect of the UK means that UK legislation sufficiently meets the EU data protection standard without the need to implement additional safeguards. This allows the transfer of personal data from the EEA to the UK to flow freely and without change.

It is important to note that the adequacy decision has a sunset provision that means this arrangement will be reviewed after 4 years. It is also possible for the European Commission to suspend or revoke the adequacy decision should UK legislation change to the extent the relevant data protection standards are no longer met. Whilst it is anticipated that any such change would be highly publicised, RSLs should continue to monitor where they are transferring data to in the event further safeguards are required.

1. Information Commissioners Office (2018) [Guide to the GDPR](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/) [↑](#footnote-ref-2)
2. UK Government (2018) [Data Protection Act 2018](http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted) [↑](#footnote-ref-3)
3. Information Commissioner (2018) [Guidance on Data Protection Fee](https://ico.org.uk/for-organisations/data-protection-fee/) [↑](#footnote-ref-4)
4. Scottish Government (2019) [Order to Extend FOISA to RSLs](http://www.legislation.gov.uk/sdsi/2019/9780111040805/contents) [↑](#footnote-ref-5)
5. Information Commissioner (2018) [Data Protection Officer guidance](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/) [↑](#footnote-ref-6)
6. National Housing Federation (2018) [Document Retention for Housing Associations](https://www.housing.org.uk/resources/document-retention-and-disposal-for-housing-associations/)

   [↑](#footnote-ref-7)
7. Scottish Council on Archives (2019) [Record Retention](https://www.scottisharchives.org.uk/resources/scarrs/) [↑](#footnote-ref-8)
8. Information Commissioner (2018) [Draft Direct Marketing Code of Practice](https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/call-for-views-direct-marketing-code-of-practice/)  [↑](#footnote-ref-9)
9. Information Commissioner [Draft Data Sharing Code of Practice](https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-consultation-on-the-draft-data-sharing-code-of-practice/) [↑](#footnote-ref-10)