PROCESSING OF SPECIAL CATEGORIES OF PERSONAL DATA AND PERSONAL DATA RELATING TO CONVICTIONS AND OFFENCES 2024

1.0 Introduction

We process special categories of personal data (SC data) and personal data relating to criminal convictions and offences (CR data) in accordance with the requirements of Articles 9 and 10 of the UK General Data Protection Regulation (UK GDPR) and Schedule 1 to the Data Protection Act 2018 (DPA 2018). This processing is undertaken for the purposes of carrying out our responsibilities as a registered social landlord in Scotland and complying with the legal and regulatory requirements that apply to us.

Some of the conditions for processing SC data and CR data contained in Schedule 1 to the DPA 2018 require us to have an Appropriate Policy Document (APD) in place. The APD must set out and explain our procedures for securing compliance with the data protection principles contained in Article 5(1) of the UK GDPR and our arrangements for the retention and erasure of such personal data. This document is our APD, explains our processing and satisfies the requirements of Part 4 of Schedule 1 to the DPA 2018. It supplements our transparency statements and Privacy Policy.

SC data is defined in Article 9 of the UK GDPR as personal data revealing:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data for the purpose of uniquely identifying a natural person;
- data concerning health; or
- data concerning a natural person's sex life or sexual orientation.

Section 11(2) of the DPA 2018 defines CR data to include personal data relating to the alleged commission of offences or proceedings for an offence committed or alleged to have been committed or the disposal of such proceedings, including sentencing.

Examples of, and information about, our processing of SC data and CR data are contained in our transparency statements.

2.0 Our conditions for processing SC data

We rely on the following conditions to justify our processing of SC data:

Condition	UK GDPR reference	Authorisation in DPA 2018
Explicit consent of the data subject obtained either in writing or verbally.	Article 9(2)(a)	Not applicable
Processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on us or the data subject in connection with employment, social security or social protection.	Article 9(2)(b)	Paragraph 1(1) of Part 1 of Schedule 1
Processing is necessary for the purposes of protecting the vital interests of the data subject or of another person.	Article 9(2)(c)	Not applicable
Processing relates to personal data which has been manifestly made public by the data subject.	Article 9(2)(e)	Not applicable
Processing is necessary for the establishment, exercise or defence of legal claims.	Article 9(2)(f)	Not applicable
Processing is necessary for substantial public interest reasons for the purposes of identifying and keeping under review the equality of opportunity or treatment between groups of people to enable such equality to be promoted or maintained. This only applies to SC data: revealing racial or ethnic origin; revealing religious or philosophical beliefs; regarding health; and relating to sexual orientation. It only concerns the following groups of people: people of different racial or ethnic origins;	Article 9(2)(g)	Paragraph 8(1) of Part 2 of Schedule 1

Condition	UK GDPR reference	Authorisation in DPA 2018
people holding different religious or philosophical beliefs; people with different states of physical or mental health; and people of different sexual orientation.		
Processing is necessary for substantial public interest reasons for the purposes of disclosing personal data to an elected representative or a person acting with the authority of such a representative in response to a communication from that representative or person.	Article 9(2)(g)	Paragraph 24 of Part 2 of Schedule 1

3.0 Our conditions for processing CR data

We rely on the following conditions to justify our processing of CR data:

Condition	Authorisation in DPA 2018
Processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on us or the data subject in connection with employment, social security or social protection.	Paragraph 1(1) of Part 1 of Schedule 1
Processing is necessary for substantial public interest reasons for the purposes of disclosing personal data to an elected representative or a person acting with the authority of such a representative in response to a communication from that representative or person.	Paragraph 24 of Part 2 of Schedule 1

Condition	Authorisation in DPA 2018
Explicit consent of the data subject obtained either in writing or verbally.	Paragraph 29 of Part 3 of Schedule 1
Processing is necessary for the purposes of protecting the vital interests of an individual.	Paragraph 30 of Part 3 of Schedule 1
Processing relates to personal data which has been manifestly made public by the data subject.	Paragraph 32 of Part 3 of Schedule 1
Processing is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings), for the purpose of obtaining legal advice or otherwise for the purposes of establishing, exercising or defending legal rights.	Paragraph 33 of Part 3 of Schedule 1

4.0 Our procedures for ensuring compliance with the UK GDPR principles

Article 5(1) of the UK GDPR sets out the data protection principles. These are our procedures for ensuring that we comply with them:

Principle 1

"*Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject*."

We ensure that we have an appropriate legal basis for processing personal data.

We process personal data fairly by ensuring that data subjects are not misled about the purposes of any processing.

We provide clear and transparent information about why we process personal data, including our lawful basis for processing, in our transparency statements and this document, which are published on our website.

Principle 2

"*Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes*."

We will only collect personal data for specified, explicit and legitimate purposes, and will inform data subjects what those purposes are in our transparency statements.

We will not process personal data for purposes incompatible with the original purpose for which it was obtained by us, unless we first inform the data subject.

If we are sharing personal data with another organisation, we will document that they must only process the personal data for the purposes contained in our transparency statements.

Principle 3

"*Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed*."

We collect and disclose the minimum personal data necessary for the relevant purposes and ensure that it is not excessive. The personal data that we process will be necessary for, and proportionate to, our purposes.

Where personal data is obtained by us, but is not relevant to our stated purposes within our transparency statements, we will erase or redact it without delay.

Principle 4

"*Personal data shall be accurate and, where necessary, kept up to date*."

We will ensure that the personal data we process is accurate and kept up to date, where necessary.

Where we become aware that personal data is inaccurate or out of date relative to the purpose(s) for which it is processed by us, we will take every reasonable step to ensure that such data is erased or rectified without delay. If we decide not to erase or rectify it, for example, because the lawful basis we rely on to process the personal data permits us to continue processing it, then we will document our decision not to do so.

Principle 5

"*Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed*."

See below under "Retention and erasure of personal data".

Principle 6

"*Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures*."

We will ensure that personal data is shared only with those who are required to see it as part of the relevant purposes specified in the transparency statements. We will, at all times, consider whether the processing or disclosure of such data is necessary for such purposes.

Appropriate organisational and technical measures are in place to protect personal data that we process. These include robust redaction processes and ensuring that personal data is only processed in line with our security procedures. Our electronic document management system and physical storage facilities within our office environment have appropriate access controls applied.

The systems we use to process personal data allow us to erase or update personal data at any point in time, where appropriate.

5.0 Accountability for compliance with the UK GDPR principles

We have put in place appropriate technical and organisational measures to meet the requirements of accountability under Article 5(2) of the UK GDPR. These include:

- The appointment of a Data Protection Officer (DPO) under Article 37 of the UK GDPR to undertake the position set out in Article 38 of the UK GDPR and to fulfil the tasks contained in Article 39 of the UK GDPR. This includes providing independent and timely advice in relation to our personal data processing, with direct access to the Chief Executive, Senior Management Team and the Board of Management, as required for fulfilment of their position and tasks.
- Taking a “data protection by design and default” approach to our personal data processing.
- Maintaining a record of our personal data processing and providing the same to the Information Commissioner’s Office (ICO) on request.
- Adopting and implementing data protection policies and procedures and ensuring we have written contracts in place with our data processors.
- Implementing appropriate security measures in relation to the personal data we process.
- Carrying out data protection impact assessments for our high-risk processing and consulting the ICO, where appropriate.

We regularly review our accountability measures and update or amend them when required.

6.0 Our arrangements for the retention and erasure of personal data

We will only retain personal data in accordance with the retention periods set out in our Data Retention Policy, which is available to data subjects on our website.

7.0 Review

This policy will be reviewed at least every 3 years, or more frequently, if necessary, in accordance with any changes in law or best practice.

This document will be retained for the duration of our processing and for a minimum of 6 months after processing of SC data and CR data ceases.

Further information

Our DPO is Daradjeet Jagpal, who can be contacted by e-mail at: ochilviewdpo@infolawsolutions.co.uk or telephone on: 07446 730475

Anne Smith
Chief Executive
24th October 2024

Policy Review and Consultation Process

Considered by the Senior Management Team on	25th October 2024
APPROVED BY THE FINANCE, AUDIT AND CORPORATE GOVERNANCE COMMITTEE ON	**7th November 2024**
APPROVED BY THE BOARD OF MANAGEMENT COMMITTEE ON	**28th November 2024**
Date of Next Review	**October 2027**