



Appropriate Policy Document

Background

The Data Protection Act 2018 (DPA 2018), Part 4 outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing special category and criminal offence data under certain specified conditions.

Almost all of the substantial public interest conditions in Schedule 1 Part 2 of the DPA 2018, plus the condition for processing employment, social security and social protection data, require Citizen to have an APD in place. (See Schedule 1 paragraphs 1(1)(b) and 5).

This document demonstrates that the processing of special categories and criminal offence data based on these specific Schedule 1 conditions is compliant with the requirements of the General Data Protection Regulation (GDPR) Article 5 principles. In particular, it refers to our retention policies with respect to this data. (See Schedule 1 Part 4).

Citizen's legal obligations

Citizen by relying on one of the Schedule 1 conditions are required to demonstrate through its general record of processing activities (included in the IRAT), under GDPR Article 30:

- (a) the condition which is relied upon;
- (b) how the processing satisfies Article 6 of the GDPR (lawfulness of processing); and
- (c) whether the personal data is retained and erased in accordance with the retention policies outlined in this APD, and if not, the reasons why these policies have not been followed.

The APD therefore complements Citizen's general record of processing under Article 30 of the GDPR and provides SC and CO data with further protection and accountability. See Schedule 1 Part 4 paragraph 41.



Description of data processed

The information detailed below is a representation of the personal data processed including special categories:

Employment data

Where Citizen needs to process SC/CO data to discharge legal obligations as an employer to ensure the health & safety of those on its premises or performing work on behalf of the organisation, or whereby an individual is obligated to provide information in connection with DBS checks or provide criminal conviction data in accordance with employment contract obligations.

- Name
- Address
- Gender
- Age (Date of Birth)
- NI Number
- Employer details
- GP details
- Working History
- Medical History (including any current conditions)
- Known drugs or alcohol use (type of drugs prescribed or otherwise, when last used drugs, quantity of alcohol use)
- Assessment and plan information including dates of referral and assessment for treatment, pregnancy status, medication, Blood-Bourne Virus status

Prevention of crime

Where Citizen needs to process CO data to prevent or detect unlawful acts and to establish whether an individual has committed an unlawful act or been involved in dishonesty, malpractice or other seriously improper conduct.

- Name
- Address

- Video images including video stills
- Location of unlawful act
- Nature of unlawful act

Protecting the public against dishonesty

Where Citizen needs to process CO data to protect members of the public from malpractice, unfitness, incompetence or mismanagement in the administration of the organisation, and obtaining consent would prejudice the exercise of the protective function.

- Processing necessary for the purposes of preventing fraud
- Processing in accordance with arrangements made by an anti-fraud organisation

Safeguarding of children and individuals at risk

Where Citizen needs to process SC/CO data in order to protect the physical, mental or emotional well-being of an individual under the age of 18, or over the age of 18 and at risk, only where in the circumstances, consent cannot be given by the data subject, cannot be reasonably obtained from the data subject, or where the processing must be carried out without the consent of the data subject because obtaining the data subject's consent would prejudice the provision of the protection, and is necessary for reasons of substantial public interest.

- Protecting vulnerable children and or an individual over the age of 18 from neglect, physical, mental or emotional harm.
- Sharing information with relevant agencies for the purpose of safeguarding

Schedule 1 condition for processing

The name and paragraph number of Citizen's relevant Schedule 1 condition(s) for processing is detailed below together with a link for the Staff and Contractor Privacy Notice:

Citizen's relevant Schedule 1 conditions for processing are:

<p>Employment, social security and social protection: Part 1 Paragraph 1 (1)</p> <p>The relevant Citizen Privacy Notices, Staff and Contractors Privacy Notice and Recruitment and Selection Privacy Notice, are located at the location below: https://www.citizenhousing.org.uk/privacy/#row1</p>
<p>Preventing or detecting unlawful acts: Part 2 Paragraph 10</p> <p>The relevant Citizen Privacy Notices , Housing Customers Privacy Notice; Citizen Young People Privacy Notice; Gateway Privacy Notice; Staff and Contractors Privacy Notice and Recruitment and Selection Privacy Notice, are located at the location below: https://www.citizenhousing.org.uk/privacy/#row1</p>
<p>Protecting the public against dishonesty: Part 2 Paragraph 11</p> <p>The relevant Citizen Privacy Notices, Housing Customers Privacy Notice; Citizen Young People Privacy Notice; Gateway Privacy Notice; Staff and Contractors Privacy Notice and Recruitment and Selection Privacy Notice, are located at the location below: https://www.citizenhousing.org.uk/privacy/#row1</p>
<p>Safeguarding of children and individuals at risk: Part 2 Paragraph 18</p> <p>The relevant Citizen Privacy Notices, Citizen Young People Privacy Notice; Housing Customers Privacy Notice and Gateway Privacy Notice are located at the location below: https://www.citizenhousing.org.uk/privacy/#row1</p>

Procedures for ensuring compliance with the principles

Citizen utilises appropriate technical and organisational controls to ensure the privacy of personal and special categories data.

Accountability principle

- i. Citizen maintain a record of our processing activities through the Information Risk Assessment Tool.
- ii. Citizen has a current suite of appropriate data protection policies.
- iii. Citizen perform data privacy impact assessments (DPIA) for uses of personal data that pose a high risk to individuals’ privacy rights.

Principle (a): lawfulness, fairness and transparency
<ul style="list-style-type: none"> i. Citizen has identified an appropriate lawful basis for processing and a further Schedule 1 condition for processing SC/CO data? ii. The Drug and Alcohol Statement 16.11.21 provides the necessary appropriate privacy information with respect to the processing of special categories data. iii. We are open and honest in the collection of special categories data and provide informed consent to staff through the Drug and Alcohol Statement 16.11.21. This ensures staff are not deceived or misled about its use.
Principle (b): purpose limitation
<ul style="list-style-type: none"> i. The Drug and Alcohol Statement 16.11.21, clearly states the purpose for processing special categories data. ii. Citizen’s Privacy Notice includes appropriate details of the purpose. iii. If we plan to use personal data for a new purpose (other than a legal obligation or function set out in law), we check that this is compatible with our original purpose or get specific consent for the new purpose.
Principle (c): data minimisation
<ul style="list-style-type: none"> i. We are satisfied that we only collect special categories personal data we actually need for our specified purposes by conducting DPIAs. ii. We are satisfied that we have sufficient special categories data to properly fulfil those purposes. iii. We will periodically review this particular special categories data, and delete anything we don’t need.
Principle (d): accuracy
<ul style="list-style-type: none"> i. We have appropriate processes in place to check the accuracy of the special categories data we collect, and we record the source of that data. ii. We have a process in place to identify when we need to keep the special categories data updated to properly fulfil our purpose, and we update it as necessary. iii. HR record, through a procedure, details of mistakes and opinions, how we deal with challenges to the accuracy of data and how we ensure compliance with the individual’s right to rectification.
Principle (e): storage limitation
<ul style="list-style-type: none"> i. Citizen carefully consider how long the special categories personal data is retained and

- we can justify this amount of time.
- ii. We regularly review our information and erase this special categories data when we no longer need it.
 - iii. We will consider the identification of any special categories data that we need to keep historical research, or statistical purposes.

Principle (f): integrity and confidentiality (security)

- i. We have analysed the risks presented by our processing through the DPIA and IRAT processes and this has influenced our assessment of the appropriate level of security required for this data.
- ii. We have an information security policy (or equivalent) regarding this special categories data and guidance. Periodic data protection audits are conducted to monitor the policy is being complied with.
- iii. We have deployed technical and organisational controls to ensure the secure processing of special categories data.

Retention and erasure policies

The special categories data is kept in accordance with our Citizen Data Retention Schedule.

Please see:

<https://www.citizenhousing.org.uk/privacy/#row4>

APD review and retention dates

Review

The Appropriate Policy Document will be reviewed by the author on or before it's third year of approval.



Retention

This APD must be retained until six months after the date Citizen stop the relevant processing. If the Information Commissioner asks to see it, it must be provided free of charge. See Schedule 1 Part 4 paragraph 40.

Version Control

VERSION	DATE	AMENDMENTS	APPROVED AT/BY	REVIEW
V 1.0	17 Jan 2022	Inclusion of crime preventions, fraud and safeguarding activities	Data Protection Officer	16 Jan 2025
[VERSION]	[DATE]	[AMEND MADE]	[NAME]	[DATE]
[VERSION]	[DATE]	[AMEND MADE]	[NAME]	[DATE]