# Privacy and data protection policy – research projects

Acuity Research & Practice Ltd is committed to protecting your privacy.

Acuity carries out research on behalf of our clients in order to help them improve services and engage with their residents. Clients provide us with personal data such as names and addresses to enable us to carry out this research.

This policy explains how the data provided to us by our clients and the data we collect as part of our research is protected by Data Protection Legislation. Acuity also has a **General Privacy and Data Protection Statement** that can be found on our website https://www.arap.co.uk/who-we-are/#policies

## 1 Research objectives

The reason for processing the data should always be clearly stated and is likely to include the following:

- To explore residents' satisfaction with their home and the services provided by their landlord
- To investigate which issues are most important to residents
- To measure satisfaction levels against the importance of issues
- To identify any new issues the landlord may not be aware of
- To feed back the results of the survey to enable the landlord to improve the services it provides
- To provide feedback to residents
- To monitor the performance of contractors

## 2 Acuity commitment to research participants

In all circumstances identities of individual respondents and their answers will be treated as confidential and will be used only for research purposes unless you expressly request or permit disclosure to a third party.

We will not mislead you.

Co-operation is voluntary at all times. Personal information will not be sought from you or about you, without your prior knowledge and agreement.

Withdrawal – at any stage you can refuse to answer specific questions. You can also ask us to destroy or delete part or all of the record of your responses. Wherever reasonable and practical we will carry out such a request.

We will not send unsolicited mail or pass on your data to others for this purpose.

If you have any further questions please contact us through the

https://www.arap.co.uk/#contact

You are welcome to check our credentials by contacting your landlord.

# 3 Data Protection Legislation

## 3.1 Interpretation

“Data Protection Legislation” means all applicable data protection and privacy legislation, regulations and guidance. This means from 25 May 2018 Regulation (EU) 2016/679 (the "General Data Protection Regulation" or "GDPR"), the Data Protection Act 2018 to the extent that it relates to processing of personal data and privacy and any national implementing laws, regulations and secondary legislation or in the event that the UK leaves the European Union, all equivalent legislation enacted in the UK in respect of the protection of personal data) and the Privacy and Electronic Communications (EC Directive) Regulations and guidance and codes of practice issued by the Information Commissioner from time to time (all as amended, updated or re-enacted from time to time).

Although the UK is no longer a member of the EU, Acuity remains fully compliant with GDPR and uses Standard Contractual Clauses for international transfers of data if required by clients within the EU.

“Data Subject”, “Personal Data Breach”, and “Data Protection Officer” take the meaning given in the Data Protection Legislation.

“Controller” - A person (who either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

“Data Processor” - Any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

“Personal Data”, - Data which relate to a living individual who can be identified – (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intention of the data controller or any other person in respect of the individual.

“Personal Customer Data” - Personal data of The Client customers processed by either the controller or The Client.

“Sub-contractor” - A sub-contractor is any individual or organisation contracted to undertake part of a project.

## 3.2 Responsibilities

For the purposes of the Data Protection Legislation, the Client is the Controller and Acuity is the Processor. The only processing that Acuity is authorised to do by the Client is listed in a schedule as part of the contract.

Acuity undertakes to process and store data in accordance with the Data Protection Legislation, the requirements of the MRS Code of Conduct and in compliance with the ISO20252:2019 standard.

The Client will ensure that any personal data used for this project will have been processed in accordance with the Data Protection Legislation.

This contract will be reviewed with any change in relevant Data Protection Legislation and any necessary amendments will be agreed in writing and appended to this contract.

## 3.3 Data Sharing

Where personal customer data is passed to Acuity, The Client will ensure that the data has been collected with appropriate data protection notifications to customers, including consent where appropriate, to enable data to be transferred to Acuity to conduct activities on The Client behalf.

Personal customer data provided by The Client will be limited to data that is required for the specific project to be conducted by Acuity and will not include any other personal data.

## 3.4 Data Transfer and Storage

The Client data including personal data and/or personal customer data will be transferred to and from Acuity by secure and encrypted means as appropriate for the type and sensitivity of the data.

Acuity will take reasonable steps as appropriate for the type and sensitivity of the data to keep the data secure and will ensure confidentiality for all employees, workers, temporary workers, agency staff, sub- contractors working on this project.

Acuity will take appropriate technical, operational and security measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Acuity uses:

- Its own in-house research applications and databases for our Computer Assisted Telephone Interviews (CATI), survey data collection and online dashboard reporting. These applications sit on Acuity's Microsoft Azure SQL databases which are cloud based, but the physical infrastructure supporting them is located in the UK South Microsoft datacenter. Microsoft operates its datacenters in a way that strictly controls physical access to the areas where our data is stored. The applications are written in Microsoft SQL, ASP and dot.net and the data is protected by layers of application level and operating system security. Access to the servers is carefully restricted and individual logins and passwords are used to ensure that users are only given access to their own data. Data files are stored in Microsoft 365, a content management platform fully compliant with the Data Protection Legislation. Data files containing client's personal and sensitive data are stored in a distinct area of the file system to which access is restricted. Acuity reviews its data storage and security on an annual basis.
- A second application supplied by Softwurk - this includes Forsta Plus for conducting Computer Assisted Telephone Interviews (CATI), survey data collection and online dashboard reporting. Forsta Plus SAAS environment is hosted with Rackspace. Forsta have a dedicated, multi-tier network security infrastructure. Data is stored on dedicated SAN arrays. Data is located in London, England. The database servers that store data are placed behind two tiers of firewalls, and data can only be accessed through the Forsta Plus applications, which is a web-based application. No application users have direct database access. The servers are only accessible for database administrators. Forsta Plus SaaS data is encrypted at rest using full SAN encryption (EMC D@RE). Individual logins and passwords are used to ensure that users are only given access to their own data. Rackspace which hosts the Forsta Plus SAAS environment has state of the art physical building security. This includes: On-site security personnel monitor the data centre buildings 24/7. Live CCTV 24/7. Biometric hand scanners are used to restrict access to the Rackspace data centre. Data files containing client's personal and sensitive

data are stored with restricted access. Acuity reviews its data storage and security on an annual basis.

Acuity will provide personal data from projects when participants have consented to the transfer to The Client and in no other instances.

When Acuity transfers personal data to The Client, in whatever form (e.g. digital, paper, recordings), the data will only be used for the purpose stated at the time it was collected. For this project this will be for research purposes and to ensure that The Client is meeting its responsibilities to their residents.

Acuity does not transfer personal data (including personal customer data) outside of the European Economic Area, or its sub-contractors, without written agreement with The Client.

## 3.5 Data Collection

When Acuity collects any information and/or personal data on The Clients behalf it will do so for purposes consistent with the proper performance of the contract.

When Acuity collects any personal data for this project it will do so as a Data Processor as agreed with The Client.

Acuity will be responsible for

- Processing data only in line with the terms of this agreement and the project scope.
- Acting only on written instruction from the Controller unless required to do so by law. The Processor is expected to inform the Client of any requirements on it to act outside of this contract in advance of undertaking the action unless they are legally unable to do so for reasons of important public interest.
- Ensuring that all people processing the data are subject to a duty of confidence.
- Taking any appropriate technical and organisational measures to ensure the security of the processing.
- The Processor must assist the Controller in meeting its obligations under subject access requests; the Controller should be notified in writing of any subject access request made to the Processor as soon as possible to allow the Controller to direct the Processor as necessary.
- The Processor must notify the Controller of a potential or confirmed data breach in writing within 24 hours.
- The processor shall submit to audits and inspections and to provide the Controller with any information needed to ensure it meets its obligations to data protection.

## 3.6 Data Retention

Acuity will retain client data for a limited period of time following completion of a project, in order that we can provide any additional reports or information requested by the client. The normal period of time for which Acuity retains personal data are 365 days for all types of records e.g. digital records, paper records, recorded data, etc. This data retention period is also included in the project specification brief. The period can be altered to meet The Client's requirements.

Acuity will ensure that any sub-contractors used for the completion of the project will retain data in accordance with agreed requirements in-line with this contract or specific written instructions of the Client.

NB: Anonymous satisfaction findings are not personal data and can be retained for the

purposes of research, benchmarking and tracking over time

## 3.7 Data Deletion and Destruction

Acuity will delete and destroy data by means as appropriate for the type and sensitivity of the data. All paper documents including questionnaires are securely destroyed with full documentation. Acuity uses Microsoft 365 to store data in a secure environment. We use a file structure to ensure that all personal and sensitive data that we store is kept in a distinct area of the file system so it can easily be identified and deleted when it is no longer needed at the end of the agreed retention period. Data deletion dates are diarised at the start of any project. Microsoft 365 allows for files to be permanently deleted so that no trace of the data remains. Acuity survey and dashboard applications are fully compliant with GDPR; no personal data is stored if it is not essential and the applications include functionality to delete all personal data when it is no longer required for the project, or if an individual requests the right to be forgotten.

Acuity will ensure that any sub-contractors used for the completion of the project will delete and destroy data in accordance with agreed requirements in line with this contract or specific written instructions of the Client.

## 3.8 Notification

Acuity shall notify the Client immediately if it:

- receives a Data Subject Access Request (or purported Data Subject Access Request)
- receives a request to rectify, block or erase any Personal Data;
- receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
- receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Agreement;
- receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or
- becomes aware of a Data Loss Event

Taking into account the nature of the processing, Acuity shall provide the Client with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made.

**Document version:**

Version: Privacy And Data Protection Statement - Research Projects 2025.Docx
Last Reviewed: 15 January 2025
Next Review: 31 December 2025