

RHA Privacy Notice - Job Applicants

Last Updated: Feb 2025
To be reviewed: Feb 2026
Approved by: Clare Murphy

Key points...

1. This privacy notice is compliant with the General Data Protection Regulations (GDPR)
2. This policy applies to all job applicants

RHA Privacy Notice - Job Applicants

Job applicant privacy notice (GDPR compliant)

RHA is aware of its obligations under the General Data Protection Regulations (GDPR) and is committed to processing applicants' data securely and transparently.

This privacy notice sets out, in line with GDPR, the types of data that is collected and held on a job applicant. It also sets out how that information is used, how long it is kept for, and other relevant information about applicants' data.

Data controller details

RHA is a data controller. This means that it determines the processes to be used when using your personal data.

Data protection principles

In relation to applicants' personal data, RHA will:

- process it fairly, lawfully and in a clear, transparent way
- collect data only for reasons that is found proper for the course of employment in ways that have been explained to the individual
- only use data in the way that the individual has been informed about
- ensure it is correct and up to date
- not keep the data for longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

Types of data RHA process

The types of applicants' data that RHA process include:

- personal details including name, address, date of birth, email address, phone numbers
- gender
- marital status
- whether or not they have a disability
- information on CVs including references, education history and employment history
- documentation relating to right to work in the UK
- driving licence

How RHA collect applicants' data

RHA collect data about applicants in a variety of ways including the information that would normally be in a CV, job application cover letter, or notes made by managers or HR during a recruitment interview.

If successful in securing a job offer, further information will be collected directly from the applicant when they complete several forms at the start of employment. Examples of this information are bank details and next of kin details. Official documentation will also be collected at this stage such as driving licence, passport, or other right to work evidence.

In some cases, data will be collected from third parties, such as employment agencies and former employers when gathering references.

Personal data is kept in a secure location within the Company's HR and IT systems.

Why RHA process applicants' data

The law on data protection allows RHA to process applicants' data for certain reasons only:

- to perform the employment contract that RHA are party to
- to carry out legally required duties
- for RHA to carry out their legitimate interests
- to protect applicants' interests
- where something is done in the public interest

All the processing carried out falls into one of the permitted reasons. Generally, RHA will rely on the first three reasons set out above to process applicants' data.

RHA need to collect applicants' data to ensure compliance with legal requirements such as:

- carrying out checks in relation to right to work in the UK; and,
- making reasonable adjustments for disabled employees.

RHA also collect data so that activities which are in the legitimate interests of the Company can be carried out. These are set out below:

- making decisions about who to offer employment to
- making decisions about salary and other benefits
- assessing training needs
- dealing with legal claims made against RHA

Applicants who are unsuccessful in obtaining employment will not have their data used for any reason other than in the ways explaining in relation to the specific application that was made.

Special categories of data

Special categories of data are data relating to:

- health
- sexual orientation
- race
- ethnic origin
- political opinion

- religion
- trade union membership and
- genetic and biometric data.

Special categories of data must be processed in accordance with more stringent guidelines. Most commonly, RHA will process special categories of data when the following applies:

- applicant has given explicit consent to the processing
- RHA must process the data to carry out their legal obligations
- RHA must process data for reasons of substantial public interest
- Applicant has already made the data public

RHA will use special category data:

- for the purposes of equal opportunities monitoring

RHA do not need applicants' consent if they use special categories of personal data to carry out their legal obligations or exercise specific rights under employment law. However, RHA may ask for consent to allow the processing of certain particularly sensitive data. If this occurs, applicants will be made fully aware of the reasons for the processing.

As with all cases of seeking consent, applicants will have full control over their decision to give or withhold consent and there will be no consequences where consent is withheld. Consent, once given, may be withdrawn at any time. There will be no consequences where consent is withdrawn.

Criminal conviction data

RHA will only collect criminal conviction data where it is appropriate given the nature of the role and where the law permits. This data will usually be collected at the recruitment stage, however, may also be collected during employment should applicants be successful in obtaining employment.

If applicants do not provide their data to RHA

One of the reasons for processing applicants' data is to allow RHA to carry out an effective recruitment process. Whilst the applicant is under no obligation to provide their data, RHA may not be able to process, or continue with (as appropriate), the applicants application.

Sharing applicants' data

Applicants' data will be shared with colleagues within the Company where it is necessary for them to undertake their duties with regards to recruitment. This includes, for example, the HR department, those in the department where the vacancy is based who are responsible for the screening of applications and interviewing, the IT department where access to our systems is required as well as undertaking any assessments requiring IT equipment.

In some cases, RHA will collect data about the applicant from third parties, such as employment agencies.

Applicants' data will be shared with third parties if successful in their job application. In

these circumstances, RHA will share their data to obtain references as part of the recruitment process/obtain a criminal records check if applicable.

Protecting applicants' data

RHA is aware of the requirement to ensure applicants' data is protected against accidental loss or disclosure, destruction and abuse and have therefore implemented processes to guard against such.

Where we share data with third parties, we provide written instruction to them to ensure that the data is held securely and in line with GDPR requirements. Third parties must also implement appropriate technical and organisational measures to ensure the security of applicants' data.

How long we keep applicants' data

In line with data protection principles, RHA only keeps applicants' data for as long as is needed. The length of time will depend on whether the applicant is successful in obtaining employment with RHA.

Applicant data will only be kept until the recruitment exercise ends in the event of:

- being unsuccessful in obtaining employment with RHA
- where RHA have not sought consent
- the applicant has not provided consent upon request to keep their data for the purpose of future suitable jobvacancies

For applicants who are successful in obtaining employment with RHA, their data will be kept and transferred to the systems RHA administer for employees. A separate privacy notice for employees will be provided to successful applicants.

Automated decision making

No decision will be made about an applicant solely on the basis of automated decision making (where a decision is taken using an electronic system without human involvement) which has a significant impact on the applicant.

Applicant rights in relation to their data

The law on data protection gives applicants certain rights in relation to the data that is held. These are:

- the right to be informed. This means that RHA must tell you how they use the applicant's data, and this is the purpose of this privacy notice
- the right of access. Applicants have the right to access the data that RHA holds on them. To do so, applicants should make a subject access request
- the right for any inaccuracies to be corrected. If any data that RHA hold on the applicant is incomplete or inaccurate, the applicant can require us to correct it
- the right to have information deleted. If the applicant would like RHA to stop processing their data, they have the right to ask RHA to delete it from their systems where the applicant believes there is no reason for RHA to continue processing it
- the right to restrict the processing of the data. For example, if the applicant believes the data RHA holds is incorrect, RHA will stop processing the data (whilst still holding it) until they have ensured that the data is correct

- the right to portability. Applicants may transfer the data that RHA hold on them for their own purposes
- the right to object to the inclusion of any information. Applicants have the right to object to the way RHA use their data where they are using it for legitimate interests
- the right to regulate any automated decision-making and profiling of personal data. Applicants have a right not to be subject to automated decision making in way that adversely affects their legal rights.

Where an applicant has provided consent to RHA use of their data, the applicant also has the unrestricted right to withdraw that consent at any time.

Withdrawing consent means that RHA will stop processing the data that the applicant had previously given RHA consent to use. There will be no consequences for withdrawing consent. However, in some cases, RHA may continue to use the data where so permitted by having a legitimate reason for doing so.

Making a complaint

The supervisory authority in the UK for data protection matters is the Information Commissioners Office (ICO). Any applicant that thinks their data protection rights have been breached in anyway by RHA are able to make a complaint to the ICO.

Data Protection Officer

RHAs Data Protection Officer is Sue Snell, Business Analyst, who can be contacted on 01733 261131.