AAGBI job applicant privacy notice

As an organisation, we are aware of our obligations under the General Data Protection Regulation (GDPR) and we are committed to processing your data securely and transparently. This privacy notice sets out, in line with GDPR, the types of data that we hold on you as a job applicant to the organisation. It also sets out how we use that information, how long we keep it for and other relevant information about your data.

This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time.

If you are offered employment with us, you should also refer to the separate workforce privacy notice.

Data controller details

The AAGBI is a data controller, meaning that it determines the processes to be used when using your personal data. Our contact details are as follows:

The AAGBI
21 Portland Place
London, W1B 1PY.

Telephone: +44 (0) **20 7631 1650**.
Email: info@aagbi.org

Data protection principles

In relation to your personal data, we will:

- process it fairly, lawfully and in a clear, transparent way
- collect your data only for reasons that we find proper for the course of your job application and in ways that have been explained to you
- only use it in the way that we have told you about
- ensure it is correct and up to date
- keep your data for only as long as we need it
- keep it securely

Types of data we process

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed.

There are ‘special categories’ of more sensitive personal data which require a higher level of protection.

We may hold many types of data about you, including:

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

How we collect your data

We collect data about you in a variety of ways including the information you would normally include in a CV or a job application cover letter, or notes made by our recruiting officers during a recruitment interview. Further information will be collected directly from you when you complete forms if you are offered employment, for example, your bank and next of kin details. Other details may be collected directly from you in the form of official documentation such as your driving licence, passport or other right to work evidence.

In some cases, we will collect data about you from third parties, such as employment agencies, former employers when gathering references or credit reference agencies.

Personal data is kept in personnel files or within the organisation’s HR and IT systems. It will also be stored on other IT systems such as email.

Why we process your data

The law on data protection allows us to process your data for certain reasons only:

- in order to perform the employment contract that we are party to
- in order to carry out legally required duties
- in order for us to carry out our legitimate interests (or those of a third party)
- to protect your interests and
- where something is done in the public interest
- where you have given your consent

All of the processing carried out by us falls into one of the permitted reasons.

We need to collect your data to ensure we are complying with **legal requirements** such as:

- carrying out checks in relation to your right to work in the UK and
- making reasonable adjustments for disabled job applicants

We also collect data so that we can carry out activities which are in the **legitimate interests of the organisation**. We have set out examples of these 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 us

Special categories of data

Special categories of data are data relating to your:

- health
- sex life
- sexual orientation
- race
- ethnic origin
- political opinion
- religion
- trade union membership and
- genetic and biometric data

We must process special categories of data in accordance with more stringent guidelines. Most commonly, we will process special categories of data when the following applies:

- you have given explicit consent to the processing
- we must process the data in order to carry out our legal obligations
- we process data for reasons of public interest, such as for equal opportunities monitoring
- where the data is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards
- you have already made the data public

Less commonly, we may process special categories of data when it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent.

We will use your special category data:

- for the purposes of equal opportunities monitoring
- to determine reasonable adjustments and to assess your fitness to work

We do not need your consent if we use special categories of personal data in order to carry out our legal obligations or exercise specific rights under employment law. However, we may ask for your consent to allow us to process certain particularly sensitive data. If this occurs, you will be made fully aware of the reasons for the processing. As with all cases of seeking consent from you, you will have full control over your 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

We will only collect criminal conviction data where it is appropriate given the nature of your role and where the law permits us (such as for DBS checks). This data will usually be

collected at the recruitment stage, however, may also be collected during your employment should you be successful in obtaining employment.

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

We may also process such information about employees or former employees in the course of legitimate business activities with the appropriate safeguards.

If you do not provide your data to us

One of the reasons for processing your data is to allow us to carry out an effective recruitment process.

We may be prevented from confirming, or continuing with, your employment with us in relation to our legal obligations if you do not provide us with information eg confirming your right to work in the UK.

Sharing your data

Your data will be shared with colleagues within the organisation where it is necessary for them to undertake their duties with regard to recruitment. This includes, for example, those responsible for HR, those in the department where the vacancy is who responsible for screening your application and interviewing you, those responsible for IT where you require access to our systems to undertake any assessments requiring IT equipment.

In some cases, we will collect data about you from third parties, such as employment agencies.

Your data will be shared with third parties if you are successful in your job application. In these circumstances, we will share your data in order to obtain references and we may share your data with others such as our payroll provider and our HR provider. You can find further information in our separate workforce privacy notice.

We do not share your data with bodies outside of the European Economic Area.

Protecting your data

We are aware of the requirement to ensure your data is protected against accidental loss or disclosure, destruction and abuse. We have implemented processes to guard against such instances and these are outlined in our Data Protection Policy.

Where we share your data with third parties, we provide written instructions to them to ensure that your data are held securely and in line with GDPR requirements. Third parties must implement appropriate technical and organisational measures to ensure the security of your data. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

How long we keep your data for

In line with data protection principles, we only keep your data for as long as we need it for and this will depend on whether or not you are successful in obtaining employment with us.

If you are unsuccessful in obtaining employment, your data will not be used for any reason other than in relation to the specific application you have made. We will retain your data for up to 12 months, in order to follow up any legal claims you may make against us.

We may seek your consent to retaining your data for up to 12 months for a secondary reason, which is in case other suitable job vacancies arise in the organisation for which we think you may wish to apply. You are free to withhold your consent to this and you will not be treated less favourably for having withheld your consent.

If your application is successful, your data will be kept and transferred to the systems we administer for employees. We will normally retain your data until six years after you leave our employment. Please refer to our separate privacy notice for employees.

Automated decision making

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

Your rights in relation to your data

The law on data protection gives you certain rights in relation to the data we hold on you. These are:

- **the right to be informed.** This means that we must tell you how we use your data, and this is the purpose of this privacy notice
- **the right of access.** You have the right to access the data that we hold on you. To do so, you should make a subject access request in accordance with our Subject Access Request Policy.
- **the right for any inaccuracies to be corrected.** If any data that we hold about you is incomplete or inaccurate, you are able to require us to correct it
- **the right to have information deleted.** If you would like us to stop processing your data, you have the right to ask us to delete it from our systems where you believe there is no reason for us to continue processing it
- **the right to restrict the processing of the data.** For example, if you believe the data we hold is incorrect, we will stop processing the data (whilst still holding it) until we have ensured that the data is correct
- **the right to portability.** You may transfer the data that we hold on you for your own purposes
- **the right to object to the inclusion of any information.** You have the right to object to the way we use your data where we are using it for our legitimate interests
- **the right to regulate any automated decision-making** and profiling of personal data. You have a right not to be subject to automated decision making in way that adversely affects your legal rights

Where you have provided consent to our use of your data, you also have the unrestricted right to withdraw that consent at any time. Withdrawing your consent means that we will stop processing the data that you had previously given us consent to use. There will be no consequences for withdrawing your consent. However, in some cases, we may continue to use the data where so permitted by having a legitimate reason for doing so.

If you wish to exercise any of the rights explained above, please speak with the recruiting manager in the first instance. There may be circumstances where we do not agree, for example to a request to have your information deleted and if this is the case, we will explain why.

Making a complaint
The supervisory authority in the UK for data protection matters is the Information Commissioner (ICO). If you think your data protection rights have been breached in any way by us, you are able to make a complaint to the ICO. You are strongly encouraged to raise any concerns first with the Data Privacy Manager, before contemplating proceeding to the ICO.

Data Privacy Manager
The AAGBI's Data Privacy Manager is Gemma Campbell, Head of Support Services & Information Management. She can be contacted at the address at the top of this privacy notice.

18 May 2018