



UK GENERAL DATA PROTECTION
REGULATION



Privacy Notice for Applicants

Thank you for sending your application form (or CV and covering letter) to the RSPCA and/or RSPCA Assured (Freedom Food Limited).

As part of any recruitment process, RSPCA and RSPCA Assured (Freedom Food Limited) collect and process personal data relating to job applicants.

Your application (or CV and covering letter) contains personal information about you and we are committed to being transparent about how we collect and use that data and meeting our data protection obligations by ensuring that this information is used only for the purpose you provided it to us, which is to assess whether you are suitable for the role which you have applied for.

Throughout this Notice we use the term “processing” to cover all activities involving your personal data, including collecting, handling, storing, sharing, accessing, using, transferring and disposing of the data.

What information do we collect?

We collect a range of information about you. This includes:

- Your name, address and contact details, including email address and telephone number(s);
- Nationality/visa (e.g. passport/driving license/national insurance numbers/birth certificate/evidence of name or gender change);
- Details of your qualification, skills, experience and employment history;
- Bank account details for salary payment purposes (if successful).
- Equity, Diversity and Inclusion (ED&I) data to enable monitoring diversity of our candidates;
- Next of kin, emergency contact and death benefit nominee(s) information.
- Whether or not you have a disability, for which we need to make reasonable adjustments during the recruitment process;
- Notes from interviews and/or assessment results e.g. psychometric test or written assessment results;
- To comply with our legal obligations or exercise legal rights conferred upon us we may collect results of pre-employment screening checks (e.g. credit history and criminal records checks where permitted by law):
 - checks for eligibility to work in the UK or EU as appropriate and as required by immigration laws, such as passport and visa documentation;
 - formal identification documentation relating to you, such as a passport or driving

- license, to verify your identity (including your date of birth);
- Disclosure and Barring Service (DBS) or Disclosure Scotland checks where we have a legal right or reason for doing so (for further information see section below);
- DVLA checks to validate driving license information if you are to drive our vehicles as part of the role applied for;
- The results of a credit check if the role requires and where we have a legal right or reason for doing so (for further information see section below);

For certain roles, we have a legal right / reason to undertake Disclosure and Barring Service (DBS) checks or in Scotland, a Disclosure Scotland check. Where we do so, we only do so in accordance with the Data Protection Laws and the prevailing legislation in the area of criminal background checks as updated from time to time. For details on how long we retain criminal convictions information and how it is disposed of, please see the section **‘How long do we keep your data’**.

We may also collect, process and store special category data about you. Special category data includes, for example, information about an individual’s racial or ethnic origin, religious or philosophical beliefs, biometric data (where it is used for identification purposes), health or sexual orientation. We will only process this where it is necessary, and any processing will be done in accordance with our obligations under relevant data protection legislation.

We may collect this information in a variety of ways. For example, data might be contained in the online application process, CVs or resumes, obtained from your passport or other identity documents, or collected through interviews or other forms of assessment.

We may also collect personal data about you from third parties, such as references supplied by former employers. We will seek information from third parties only once a job offer to you has been made and will inform you that we are doing so.

We use the external Applicant Tracking System called eArcu to manage and process applications for job vacancies. This is a third party service provided by eArcu, Davenport House, Bowers Way, Harpenden, England, AL5 4HX, to whom applicant data will consequently be transferred. If / when applicants use the eArcu platform to manage or submit an application, the [Privacy Notice of the eArcu](#) also applies. eArcu will use personal information of applicants solely for the processing of applications.

For some of our vacancies, we use third parties such as recruitment agencies, sourcing tools and headhunters, to find candidates. If you approach or are approached by one of these third parties and you decide to apply, these third parties will share your application data with us.

Also, when you apply via a referral, the person referring you will upload your contact details and CV (potentially other data you have provided to this person) in our applicant tracking system. We will always notify you via email after such data is received from referrals or third parties and will then send you this privacy notice. We will also notify you if we need any more information from you to be able to progress your application.

Why do we process personal data?

We need to process data to take steps at your request prior to entering into a contract with you. We may also need to process your data to enter into a contract with you.

In some cases, we need to process data to ensure we are complying with our legal obligations. E.g. check for eligibility to work in the UK.

We have a legitimate interest in processing personal data during the recruitment process and for keeping records of the process. Processing data from job applicants allows us to manage the recruitment process, assess and confirm a candidate's suitability for employment and decide to whom we offer a job. We may also need to process data from job applicants to respond to and defend against legal claims.

We may process special categories of data, such as information about ethnic origin, sexual orientation or religion or belief, to monitor recruitment statistics. We may also collect Equity, Diversity and Inclusion (ED&I) data for diversity and inclusion purposes, information about whether or not applicants are disabled to make reasonable adjustments for candidates with a disability. We would process such information to carry out our obligations and exercise specific rights in relation to employment.

We process this data we collect from these sources to assess your suitability for the relevant positions with us and therefore for our legitimate interests of being able to administer and manage our recruitment process and make sure the right people end up in the right roles.

We sometimes use data we gather during the application phase to carry out statistical analyses of our successful applicants, for example to see which (university) degrees our successful applicants often hold. We use these statistics, which are never kept in any way that allows for identification of individuals, to optimize our recruitment strategy. If necessary, we can also use your information for our legitimate interest of protecting our legal rights, for example in connection with legal claims, and when we have a legal obligation to do so.

Where is the data stored?

Data may be stored in a range of different places, including in your application record, on the external Applicant Tracking System, in HR management systems and on other IT systems including email.

Who has access to data?

Your information may be shared internally for the purposes of the recruitment exercise. This includes members of the HR and Resourcing team, interviewers involved in the recruitment process, managers in the business areas with a vacancy and IT staff members, if access to the data is necessary for the performance of their roles.

When you apply for a role with RSPCA / RSPCA Assured, this is via the recruitment platform of the external Applicant Tracking System eArcu which manages and processes the applications for job vacancies.

Access to the data stored in the Applicant Tracking System is restricted to the recruitment /resourcing managers and / or officers, managers in relevant areas and Human Resources.

With whom do we share data?

Where necessary so we can administer and manage our recruitment process, we will share your information with our service providers and professional advisers (e.g. recruitment agencies, providers who carry out screenings on our behalf, and, if applicable to the position you are applying for, suppliers who run candidate assessment programmes for us). We have concluded agreements with our service providers to protect your personal data.

As mentioned above, we will also contact third parties including those whose details you have supplied (referees) so that we can verify information you have provided us in relation to your previous employment and qualifications.

We will not share your information with any third party, unless we have your permission, where this is necessary in connection with the purposes above, for protecting our legal rights or when we have a legal obligation to do so.

We do not transfer your data to any countries outside the UK.

How do we protect data?

We take the security of your data seriously. We have internal policies and controls in place to ensure that your data is not lost, accidentally destroyed, misused or disclosed and is not accessed except by our employees in the proper performance of their duties.

How long do we keep your data?

We keep your personal data and special category personal data securely for as long as it is legitimately required or necessary to fulfill the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Information about how long we retain such personal data is set out in the table below:

Data category	Retention Period	Reason	Disposal
Job applications and interview records of candidates	12 months - unless following an unsuccessful application you specifically consent to us holding it for longer for the purpose of contacting you in the event that any similar jobs / roles become available. from time to time.	To defend against potential legal claims.	Securely destroyed by a third party.

Criminal Records Information (such as DBS check results)	6 months	To comply with the DBS code of practice issued under section 122(2) of the Police Act 1997.	Securely destroyed by a third party.
---	----------	---	--------------------------------------

Should your application be unsuccessful, your personal information will be securely destroyed after 12 months. If your application is successful, your personal data will be held in line with the Privacy notice for employees, workers and contractors. This will be provided to successful candidates as part of onboarding processes, or you can also request a copy sooner by emailing the HR department (hrd@rspca.org.uk).

You have the right at any time to withdraw your consent for us to process your personal information and, if you wish to withdraw your consent, please email hrd@rspca.org.uk. Once we have received notification that you have withdrawn your consent, we will no longer process your application and we will dispose of your personal data securely.

Your rights

You are entitled to object to us processing your personal data. You may also ask us for an overview of your information or ask for a copy. You may also request us to correct or delete certain data, restrict processing of your data, or ask us to transfer some of this information to other organizations. In some cases you may object to the processing of your data and, where we have asked for your consent to process personal data, you can withdraw this consent at any time. Where we process your data for our legitimate interests, you can contact us if you want more information about these legitimate interests.

There are some exceptions to these rights, however. For example, it will not be possible for us to delete your data if we are required by law to keep it or if we hold it in connection with a contract with you. Similarly, access to your data may be refused if making the information available would reveal personal information about another person or if we are legally prevented from disclosing such information.

If you would like to exercise any of these rights, please contact our Data Protection team at data.protection@rspca.org.uk.

If you believe that RSPCA/RSPCA Assured has not complied with your data protection rights, you have the right to complain to the [Information Commissioner](#).

What if you do not provide personal data?

You are under no statutory or contractual obligation to provide data to RSPCA/RSPCA Assured. However, if you do not provide the information, we may not be able to process your application properly or at all.