

**GDPR TEMPLATE:**

**JOB APPLICANT PRIVACY NOTICE**

**Points to note**

* Before using this template Job Applicant Privacy Notice, it is essential that you read these ‘Points to note’, together with the separate document, ‘Make UK Essential GDPR Templates for HR – Points to note’, which provides important information applicable to all of the template documents, including the Job Applicant Privacy Notice.
* The GDPR requires you to be transparent with individuals whose personal data you process and provide them with required information about your processing activities, i.e. to explain to them what you do with their personal data. This template Privacy Notice is designed to comply with this requirement in respect of Job Applicants (as defined in the body of the document). There is a detailed list of information that must be included in the Privacy Notice, all of which is covered in this template.
* This template is for the Job Applicant Privacy Notice, so it covers what you do with Job Applicants’ personal data during an active recruitment process and what you do at the end of that process with the personal data of unsuccessful Job Applicants and successful Job Applicants who do not accept the job they are offered. (Successful Job Applicants who accept an offer of employment should receive the Employee Privacy Notice as part of their induction. Information about the recruitment data that you keep once someone joins you is therefore covered in that document).
* The template takes into account the (somewhat conflicting) GDPR requirements for a privacy notice to give detailed, specific information to individuals, and to provide it in a concise, intelligible, accessible form. We have taken a ‘middle ground’ approach to the level of detail we have included in the document, and we have sought to aid Job Applicants’ understanding by dividing the information it covers into easily digestible sections using headings for signposting wherever possible.
* There is no ‘one size fits all’ when it comes to producing an organisation’s Job Applicant Privacy Notice. We have included details of the types of personal data we think most employers will hold and process about Job Applicants. However, each employer must consider what is to be included in the context of its own business requirements/operations. It is therefore essential that you customise the template Job Applicant Privacy Notice to reflect the types of personal data that you hold and how you process them. (The results of any audit you have conducted will help you to do this).
* Note that this template Job Applicant Privacy Notice is intended to comply with the requirements of the UK GDPR and DPA 2018. It is suitable for UK-based employers to issue to Job Applicants in the UK. If you are a UK-based employer that is recruiting Job Applicants to work in the EEA, you are likely to remain subject to the EU GDPR and will need to provide an EU GDPR compliant privacy notice to those individuals. A privacy notice that complies with the EU GDPR would need to include the details of your EEA representative if you do not have an office or establishment in the EEA. (See the ICO’s guidance for details of the requirement to appoint an EEA representative: <https://ico.org.uk/for-organisations/data-protection-and-the-eu/data-protection-and-the-eu-in-detail/the-uk-gdpr/european-representatives/>.) There may also be other requirements for the content of a privacy notice under local law in the EEA country where you are recruiting, so we recommend that you take advice on your particular circumstances.
* **Personal data concerning criminal offences*:*** We have included optional wording about obtaining criminal offences/criminal records data at shortlisting or offer stage in the special category data section of this Privacy Notice. (Note that data relating to criminal offences/criminal records is not considered special category data under the UK GDPR, but we have dealt with it in the section of this Privacy Notice concerning special category data because similar restrictions apply to its processing under the DPA 2018.) If you do not seek data about criminal offences/criminal records from any Job Applicants, you should delete this section.
* Unfortunately, the GDPR makes it very difficult for employers to request criminal records information from Job Applicants and/or require them to undergo DBS checks. We explain the position in detail below, but in very brief summary:
  + You might be able to justify conducting criminal record checks for some limited roles in your organisation, but this will very much depend on the nature of the role.
  + In all cases, you should only conduct checks where this is really necessary and you should do it at as late a stage in the recruitment process as possible.
  + It is not possible to rely on consent as a legal basis for processing criminal records data in the context of recruitment, and it may be difficult to find alternative legal bases.
* The first issue to consider is to identify the purpose of your processing, i.e. the reason why you need to conduct criminal record checks / ask for disclosure of criminal offences. According to guidance on processing criminal offences data produced by the ICO in partnership with ‘Unlock’, to obtain a criminal records check under the GDPR, you must define the purpose for which you require the criminal offences/criminal records data and be able to demonstrate that there is a clear and rational link between obtaining the information and fulfilment of that purpose. If you can achieve the purpose another way, then obtaining the criminal offences/criminal records data is not **necessary** and will not comply with the GDPR. Indeed, this point on necessity is reinforced in the ICO’s detailed guidance on processing criminal offences/criminal records data.
* To process criminal offences/criminal records data, there will need to be both an ordinary legal basis and also an additional criminal offences/criminal records legal basis. It is not possible to rely on consent as a legal basis for processing criminal records data and, as set out below, it may be difficult to find alternative legal bases. (Under the GDPR, consent is not considered to be freely given where there is an imbalance of power in the relationship between the parties – as would be the case where a Job Applicant is told that if they do not consent to disclosing convictions and/or getting a DBS check, they will not be offered the job.)
* The legal bases that you rely on will vary, depending on whether the job is on the list of excepted occupations under the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975. If none of your jobs are on the excepted occupations list, you should delete the wording relating to the Rehabilitation of Offenders Act and excepted occupations. This online tool on the Government website should enable you to establish whether any of the jobs in your organisation are on the excepted occupations list: <https://www.gov.uk/find-out-dbs-check>.
* Where a job is on the list of excepted occupations under the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975, an employer may be able to establish that their ordinary legal basis for requiring criminal records checks is that this is necessary for compliance with a legal obligation, e.g. if the Job Applicant will be working with vulnerable people and the employer is therefore subject to safeguarding obligations, or if the Job Applicant will be working in an area in which staff must be vetted for national security reasons.
* However, this legal basis may not be applicable for all jobs on the excepted occupations list. Where there is no legal obligation to carry out a criminal records check, or where the job is not even on the list of excepted occupations, an alternative ordinary legal basis for the employer may be that the processing is necessary in their legitimate interest to protect their business and its customers from risk, e.g. of dishonesty/theft. (However, employers would only be able to rely on this if their interest is not outweighed by the individuals’ rights and freedoms – here, the right of someone who has served their sentence to live and work without continuing punishment for their earlier crime. For example, if the role in question isn’t one that involves handling significant customer payments, then it is arguable that employers could achieve their purpose sufficiently by interviewing applicants to form their own view of their personality and obtaining references from past employers as to their character. In this regard, the ICO’s detailed guidance on processing criminal offences/criminal records data flags that you would need to carry out a legitimate interests assessment (LIA), taking into account the particular risks associated with processing criminal offences/criminal records data, in order to determine whether you can rely on the legitimate interests legal basis. A template LIA is available on the ICO website: <https://ico.org.uk/media/for-organisations/forms/2258435/gdpr-guidance-legitimate-interests-sample-lia-template.docx>).
* As to the additional legal basis for processing criminal records data, there is the argument that employers have a legal obligation in relation to employment that enables them to seek criminal records data for Job Applicants for positions on the excepted occupations list. Where there is no applicable legal obligation, the employer could say that inclusion of the job on that list gives it a legal *right* to obtain the check, but this is as yet untested. In any event, the wording in this Privacy Notice refers to ‘legal right/obligation in relation to employment’ as the additional legal basis for processing criminal records data where the job in question is on the list of excepted occupations. It also references the prevention or detection of unlawful acts, which might also be appropriate as an additional legal basis where there is no applicable legal obligation for the employer to obtain the check for positions on the excepted occupations list. (See below for further discussion of ‘the prevention or detection of unlawful acts’ legal basis.)
* Most jobs in the manufacturing sector are unlikely to be on the excepted occupations list and, for jobs that are not on the list, the only way to obtain criminal records information is to ask the Job Applicant to disclose convictions, or to seek a basic DBS check for him/herself or via a third party vetting company that has been approved as a ‘Responsible Organisation’ by the DBS and pass the result to the employer. Employers who want to seek criminal offences/criminal records data in these circumstances are in a difficult position. Even if they are able to establish legitimate interests as an ordinary legal basis for processing the data, they may struggle to identify an appropriate *additional* legal basis for processing.
* In accordance with the ICO guidance, the wording in this Privacy Notice identifies the prevention or detection of unlawful acts as an additional legal basis for processing Job Applicants’ criminal records data for jobs that are not on the excepted occupations list. However, it is important to note that, this additional legal basis would only be applicable where there is a potential risk of unlawful behaviour in employing someone with a criminal record – and it would be for the employer to be able to demonstrate this. It is therefore sensible only to seek criminal records information for certain Job Applicants, e.g. those whose positions involve significant financial responsibility or handling large customer payments, where the employer might be more likely to be able to demonstrate the risk involved in employing someone with a criminal record. (Note, the ICO guidance makes clear that (unlike for other special category data) there is no need to establish a public interest when relying on this additional legal basis to process criminal offences/criminal records data.)
* Some employers might choose to tailor this Privacy Notice and state that consent is their additional legal basis for processing Job Applicants’ criminal records data, but this approach is not compliant with the GDPR and employers who take this approach will need to weigh up the risks involved. (If you will only seek criminal offences/criminal records data for jobs on the excepted occupations list and will do so only by requesting standard or enhanced checks from the DBS, you should delete the references to self-disclosure and basic DBS checks).
* **Sharing Job Applicants’ personal data:** We have included optional wording to cover situations where you share Job Applicants’ personal data with third parties. The most common examples are recruitment agencies, your own parent/group companies, referees, and background checking service providers. Where such third parties are data controllers in their own right, they would ordinarily have to provide their own privacy notice to the Job Applicants whose personal data they obtain from you. However, there is an exception to this requirement where they obtain the personal data from someone other than the data subject (i.e. from you, rather than from the Job Applicant directly) and the data subject already has the relevant fair processing information. In order to ease the administrative burden for group companies, we have therefore included optional language that should avoid those companies having to provide your Job Applicants with their own privacy notice. You should use this language where you routinely share Job Applicants’ personal data with your parent/group company to obtain their input on the recruitment selection process. (Note also that if you share Job Applicants’ personal data with your parent/group company not just to get its input in your recruitment process, but also for the purposes of considering the Job Applicant for alternative roles at the parent/group company, you should obtain the Job Applicant’s consent to be put forward for such roles, and the parent/group company would then need to issue its own privacy notice to the Job Applicant).
* **Transfers outside the UK:** The obligation to inform Job Applicants about transfers of their personal data outside the UK only applies where such transfers do actually take place. This section of the template Privacy Notice is therefore in square brackets as, if you do not transfer any Job Applicant personal data outside the UK, you will not need to include it. However, you will need to take care that you update the Privacy Notice if you introduce such transfers in the future.

The UK GDPR restricts the transfer of personal data to countries outside the UK unless certain the country is recognised as providing adequate protection for personal data, appropriate safeguards are in place, or an exception applies. If you currently transfer Job Applicant personal data to any countries outside the UK, you must identify those countries and provide details of the relevant arrangements:

* + With regard to transfers of personal data from the UK to the EEA, the UK Government’s has recognised the adequacy of data protection provisions in EEA countries. Accordingly, this template Privacy Notice assumes that personal data can flow freely from the UK to the EEA.
  + For transfers of personal data from the UK to other countries, the UK Government has recognised the effectiveness of existing European Commission adequacy decisions, so transfers to those countries can continue. (Going forwards, the UK can make its own adequacy decisions. So far, an adequacy decision has been issued in respect of the Republic of Korea (South Korea). In addition, adequacy has been confirmed in respect of organisations in the USA that have signed up to the UK Extension to the EU-US Data Privacy Framework – a binding set of commitments that are enforced in the USA by the Federal Trade Commission.) Transfers to other countries that do not have an adequacy decision (or to organisations in the USA that have not signed up to the UK Extension to the EU-US Data Privacy Framework) require you to conduct a transfer risk assessment and put appropriate safeguards in place, such as the ICO’s International Data Transfer Agreement (IDTA) or its UK Addendum to the EU standard contractual clauses, or binding corporate rules if the transfer is between group companies. Please refer to the ‘Make UK Essential GDPR Templates for HR – Points to note’ for further information on transfer risk assessments and appropriate safeguards.

We have assumed that the most common circumstances in which employers will transfer Job Applicants’ personal data outside the UK is if they transfer the personal data to a parent/group company that is based outside the UK and is somehow involved in the recruitment process, so we have included template wording specifically to cover such transfers. We have also added some generic template wording covering transfers to other recipients outside the UK. Both sets of wording will need to be tailored to reflect your practices.

Finally, note that this template Privacy Notice is written from the perspective of a UK-based company, rather than a company based in the EEA or elsewhere, so it provides information about transfers of Job Applicant personal data out of, rather than into, the UK. For further information about transfers of personal data into the UK, please refer to the ‘Make UK Essential GDPR Templates for HR – Points to note’.

* **Referees:** The personal details of referees (e.g. name, address, phone number) are personal data and, in order to comply with the GDPR, you should provide referees with required information about your processing activities. We have included wording in the Job Applicant Privacy Notice telling Job Applicants that they must let their referees know what personal data they are providing to you and must give their referees your contact details. However, this does not satisfy the requirement for you to provide the required information to the referees. As you will receive referees’ personal data from Job Applicants, rather than from the referees themselves, you must provide this information within a reasonable period, and at the latest within one month, of receiving their personal data. If you request referees’ details on the initial application form, and it will take more than a month before you seek references, to be properly compliant, you would need to provide referees with fair processing information before this. By contrast, if you only request referees’ details from Job Applicants at a late stage of the recruitment process (e.g. at short-listing, or when making a job offer), then you will most likely be seeking references within one month of receiving the referees’ details, so providing them with the required information at the point when you request a reference should be sufficient. To reduce the administrative burden of providing the required information to referees, you may wish to consider deleting: the personal data of any referee you do not intend to request a reference from; and any referee data from CVs/job applications you receive which you intend to keep on file (see below).
* **Keeping data on file:** It is quite common for employers to wish to keep some Job Applicants’ details on file (e.g. if they submitted a speculative application or were unsuccessful for the job they applied for, but the employer still thinks they could be a promising candidate for future vacancies). The GDPR does not prohibit this, but you will need to consider your legal basis for doing so. In our view, this is one of the rare occasions on which consent would be an appropriate legal basis for employers to rely upon. Provided you allow Job Applicants to apply for a given vacancy *without* also consenting to having their details kept on file, and this does not impact on your consideration of their current application, you can be comfortable that their consent is freely given. In this Privacy Notice, we have included wording to inform Job Applicants that their details will be kept on file for consideration for future vacancies on this basis. If you do wish to keep Job Applicants’ details on file with their consent, you will need to consider how best to obtain that consent. This will depend on how you present and implement the Job Applicant Privacy Notice (see below).

**Points to note – presentation and implementation**

* As with the main Employee Privacy Notice, we have presented the Job Applicant Privacy Notice in a text/print-out format. However, depending on your organisation’s technological capabilities, it could be presented in a more user friendly form. In addition, the guidance to the GDPR requires you to consider the most appropriate medium (hard copy, online on your company intranet, etc.) for privacy notices, based on what the individual will most easily be able to access in the circumstances.
* How you present the Job Applicant Privacy Notice will necessarily depend on how you receive job applications:
  + If you invite Job Applicants to apply via an online form on your website or a recruitment portal, it would be appropriate to present the Job Applicant Privacy Notice online – ideally as a screen the applicant would have to read through before being able to click “submit” to send you their application. You should also ensure that the Job Applicant is able to access the Privacy Notice easily after they have sent their application through to you, in case they want to refer to it again. (If you wish to seek the Job Applicant’s consent to your keeping their details on file, you could include appropriate consent wording and a tick box for them to check on another page of your online form).
  + If you ask Job Applicants to send their CV/application form to a dedicated recruitment email address, you could set this up so that it generates an automated reply acknowledging receipt and attaching a copy of, or providing a link to, the Job Applicant Privacy Notice. This would work both for applications for specific vacancies, and unsolicited/speculative applications. (If you wish to seek the Job Applicant’s consent to your keeping their details on file, you could state in the automated response that the Job Applicant should reply to that email to give their consent to this).
  + If you use a recruitment agency to source suitable candidates, you should require the recruitment agency to provide the Job Applicant Privacy Notice (in soft or hard copy) to any candidate whose details they send you. Recruitment agencies should generally not send candidates’ details to you unless the candidate has agreed to this – so a logical stage of the process to give the candidate your Job Applicant Privacy Notice would be when the recruiter tells the candidate about the vacancy in your organisation and asks the candidate if they would be interested in being put forward. (If you wish to seek the Job Applicant’s consent to your keeping their details on file, you could ask the recruitment agency to get the Job Applicant to sign a consent form, which the agency would then forward on to you together with the Job Applicant’s details).
* You must also consider whether/how you will provide the Job Applicant Privacy Notice to people who send you speculative/unsolicited hard copy applications:
  + If an application or CV is sent by post/handed in, and you don't put it into any sort of a filing system and don't intend to, then it isn't personal data so it is out of scope. So, if HR look at it and then shred it without scanning it/filing it, then there is no need to provide a privacy notice.
  + If HR do scan or file the application or it is sent electronically, then it is personal data, and the obligation to provide a privacy notice will apply. There is unfortunately no exception for unsolicited information. So, strictly speaking, to comply with the GDPR requirements, you should email or post a copy of your Job Applicant Privacy Notice back to the individual – you could do this in conjunction with a communication acknowledging receipt of the application.
  + If you do not want to do this, then you could include privacy notice information about unsolicited applications on your website, preferably in the section of the website that covers recruitment and job applications. It is better to do something than nothing. This is, however, unlikely to be enough to satisfy the obligation to 'take appropriate measures' to provide privacy notice information as required under the GDPR – the ICO may take the view that sending a quick email attaching a copy of/providing a link to the Job Applicant Privacy Notice or putting a copy in the post is not a big burden.
  + That said, companies will of course be making risk based decisions about compliance. The risks here may not be that high – it is a breach not to provide the privacy notice, but the level of risk will depend on who sends CVs to you. If an individual is keen to make trouble, and you don't send a privacy notice back, they can complain to the ICO, who may investigate but – we think – would be more likely to tell you to change your practice going forward than to issue a fine straightaway. A troublesome individual may also bring a claim against you in court. In most cases, it would be difficult for the individual to claim much damage, but it would still be a nuisance.

**Job Applicant Privacy Notice**

This Job Applicant Privacy Notice sets out what personal data we, [COMPANY], hold about you and how we collect and use it during and after the recruitment process. It applies to anyone who is applying to work for us, whether as an employee, worker, [*contractor, consultant, intern, volunteer, partner or director*] (together referred to as ‘Job Applicant’ or ‘you’).

Please note that we will not necessarily hold, use or share *all* of the types of personal data described in this Privacy Notice in relation to you. The specific types of data about you that we will hold, use and share will depend on the role for which you are applying, the nature of the recruitment process, how far you progress in the recruitment process and your individual circumstances.

We are required by data protection law to give you the information in this Privacy Notice. It is important that you read the Privacy Notice carefully, together with any other similar or additional information that we might give you from time to time about how we collect and use your personal data. Should your application be successful, when you start work for us, we will provide you with another privacy notice that explains how we deal with your personal data whilst you are working for us and after you have left.

This Privacy Notice applies from [date], and supersedes any previous versions. It does not give you any contractual rights. We may update this Privacy Notice at any time.

**Who is the controller?**

[*Name employer*] is the “controller” for the purposes of data protection law (also referred to in this notice as ‘we’ or ‘us’). This means that we are responsible for deciding how we hold and use personal data about you. We can be contacted as follows: [*Contact details*].

[*If you have a Data Protection Officer*: Our Data Protection Officer is [*name and contact details*]. As Data Protection Officer, they are responsible for informing and advising us about our data protection law obligations and monitoring our compliance with these obligations. They also act as your first point of contact if you have any questions or concerns about data protection].

**What is personal data?**

Personal data means any information relating to a living individual who can be identified (directly or indirectly), in particular by reference to an identifier (e.g. name, NI number, employee number, email address, physical features). It can be factual (e.g. contact details or date of birth), an opinion about an individual’s actions or behaviour, or information that may otherwise impact that individual in a personal or business capacity.

Data protection law provides additional protection for personal data about an individual’s racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health, sex life or sexual orientation, criminal convictions or offences, biometrics (if used for identification purposes), or genetics. This is referred to as **special category** **data**. (We refer to personal data that is not special category data as **ordinary personal data.**)

**What type of ordinary personal data do we hold about you and why?**

At the initial stages of recruitment, we collect, hold and use the following types of ordinary personal data about you:

* Information contained in your application form/CV/covering letter, including your name, title, contact details, [photograph], employment history, experience, skills, qualifications/training (including educational, vocational, driving licences where appropriate), referees’ names and contact details, etc.
* Publicly available information about you, such as your business social media presence.
* Selection information, including correspondence, interview notes, internal notes, the results of any written or online selection tests.

If you are shortlisted for a position, or you receive a conditional offer of employment, we may collect, hold and use the following additional types of ordinary personal data about you:

* Pre-employment check information, including references and verification of qualifications
* Right to work checks and related documents

We hold and use this personal data so that we can:

* process your application and correspond with you about it;
* assess whether you have the required skills, experience, qualifications and training for a role within the company;
* make informed recruitment decisions;
* verify information provided by you;
* check and demonstrate that you have the legal right to work in the UK;
* keep appropriate records of our recruitment process and decisions;
* [*insert any additional purposes*].

**What are our legal grounds for using your personal data?**

Data protection law specifies the legal grounds on which we can hold and use personal data.

We rely on one or more of the legal grounds set out below when we process your personal data. (Note that, where we are processing special category data, we will have an additional legal ground as well – see below, **What type of special category personal data do we hold about you, why, and on what legal grounds?**)

* We need it to take steps at your request in order to enter into a contract with you (**entry into a contract**), because by applying for a job with us you are effectively asking us to enter into a contract with you [whether this is an employment contract, a contract for services or another type of contract].
* We need it to comply with a legal obligation (**legal obligation**), e.g. the obligation not to discriminate during our recruitment process, or the obligation not to employ someone who does not have the legal right to work in the UK.
* It is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests (**legitimate interest**). For example, it is in our legitimate interests to review and consider your personal data (as listed above) so that we can select the most appropriate candidate for the job.

**What type of special category personal data do we hold about you, why, and on what legal grounds?**

We will only collect, hold and use limited types of special category data about you during the recruitment process, as described below.

Since special category data is usually more sensitive than ordinary personal data, we need to have an additional legal ground (as well as the legal grounds set out above – **What are our legal grounds for using your personal data?**) to collect, hold and use it. The additional legal grounds that we rely on to collect, hold and use your special category data are explained below for each type of special category data.

At the initial stages of recruitment, we collect, hold and use the following special category data about you:

**Equal opportunities monitoring**

Equal opportunities monitoring data which could include information about your race or ethnicity, religious beliefs, sexual orientation or health. We use this information to monitor equality of opportunity and diversity in our recruitment process. Our additional legal ground for using this information is that it is necessary in the public interest for the purposes of equal opportunities monitoring and is in line with our Data Protection Policy.

**Adjustments for disability/medical conditions**

Information relevant to any request by you for adjustments to the recruitment process as a result of an underlying medical condition or disability. We use this information to enable us to carry out a fair, non-discriminatory recruitment process by considering/making reasonable adjustments to our process as appropriate. Our additional legal ground for using this information is that we need it to comply with a legal obligation/exercise a legal right in relation to employment – namely, the obligations not to discriminate, and to make reasonable adjustments to accommodate a disability – and such use is in line with our Data Protection Policy.

[*If you collect further special category data after shortlisting/conditional offer:* If you are shortlisted for a position, or you receive a conditional offer of employment, we may collect, hold and use the following additional types of special category personal data about you:

[*If applicable:* **Pre-employment health questionnaires/medicals**

We collect information about your health in a pre-employment medical questionnaire and/or examination, as well as any information about underlying medical conditions and adjustments that you have brought to our attention. We use this information to assess whether you are fit to do the job with adjustments, to consider/arrange suitable adjustments and to comply with health and safety requirements. Our additional legal grounds for using this information will usually be that we need it to comply with a legal obligation/exercise a legal right in relation to employment – namely, the obligation to make reasonable adjustments to accommodate a disability – and such use is in line with our Data Protection Policy.]

[*If applicable:* **Criminal records information/DBS checks**

[Where you are applying for a job that is on the excepted occupations list under the Rehabilitation of Offenders Act 1974, we may request criminal records checks from the DBS.] We may ask you to disclose if you have any criminal convictions and/or we may ask you to seek a basic criminal records check from the DBS [via a third party vetting company] and disclose the results to us. Where we seek this information, we use it to assess your suitability for the role and this is necessary because [*insert further detail of purpose, explaining* ***why*** *you need the criminal records information to assess suitability for the roles in question*]. [For jobs that are on the excepted occupations list, our additional legal ground for using this information is that it is necessary for compliance with a legal obligation/exercise of a legal right in relation to employment and/or that it is necessary for the prevention or detection of unlawful acts (and we process it in accordance with an appropriate policy document). In all other cases, our][Our] additional legal ground for using this information is that it is necessary for the prevention or detection of unlawful acts (and we process it in accordance with an appropriate policy document).]

**How do we collect your personal data?**

You provide us with most of the personal data about you that we hold and use, for example in your written application, by completing any assessments and during any interviews.

Some of the personal data we hold and use about you is generated from internal sources during the recruitment process. For example, [the person interviewing you may score your suitability for the role and we record the reasons for decisions made about whether or not your application is successful.]

Some of the personal data about you that we hold and use may come from external sources. [*If you use a recruitment agency to shortlist candidates:* For example, a recruitment agency provides us with a shortlist of candidates.] If we offer you a role, we will carry out pre-employment checks, such as taking up references from past employers or education providers [*if you check qualifications from awarding bodies:* and we may check your qualifications by contacting the awarding body.] [*If you will ask the successful candidate to undergo a medical*: We may ask an occupational health professional to report to us on your fitness to do the job.] [*If you will ask a successful candidate for a job on the excepted occupations list for a DBS check:* We may seek a criminal record check from the DBS.] [*If you engage a third party vetting company to conduct background checks and/or seek basic DBS checks:* We use a third-party provider to conduct [limited background checks] [[and] basic criminal record checks] on successful Job Applicants.] In some circumstances, we may ask the Home Office for information about your immigration status to verify your right to work in the UK. For some roles, we may also obtain information about you from publicly available sources, such as your LinkedIn profile or other media sources.

**Who do we share your personal data with and on what legal grounds?**

[*If you share Job Applicants’ personal data with a parent/group company:* **Parent/group companies**

We share any of your personal data that is relevant, where appropriate, with our [parent/group] company, [*name parent/group company*], to [enable them to input into the recruitment process and approve final recruitment decisions/*insert other applicable reason*]. Our legal grounds for doing so are that: it is necessary for entry into a contract; and/or it is in our legitimate interest to [obtain our [parent/group] company’s approval of our recruitment decisions and comply with the procedures applicable within our corporate group].

*If you always share personal data with parent/group company to obtain their input on the recruitment process, also include the following (see Points to note):* This Privacy Notice also covers how [*name of parent/group company*] uses any personal data about you that we share with them. [*Name of parent/group company*] is the controller of any personal data they hold and use about you and their contact details are [*insert contact details*]. [*If the parent/group company has a Data Protection Officer*: The [*name of parent/group compa*ny’s] Data Protection Officer is [*name and contact details*]. As Data Protection Officer, they are responsible for informing and advising [*name of parent/group company*] about its data protection law obligations and monitoring its compliance with those obligations. They also act as your first point of contact if you have any questions or concerns about data protection in relation to the personal data they hold]. [*Name of parent/group company*] applies the same high standards to data protection compliance as we do.]]

[*If you use recruitment agencies:* **Recruitment agencies**

We engage recruitment agencies to [provide us with the details of suitable candidates for our available vacancies, to communicate with those candidates, to handle administration in connection with the recruitment process[, *insert other functions*]. If we have received your initial application details from a recruitment agency, we will share with them any of your personal data that is necessary to enable them to fulfil their functions for us. Our legal grounds for doing so are that: it is necessary for entry into a contract; and/or it is in our legitimate interest to engage service providers to assist us with the recruitment process.]

**Medical/occupational health professionals**

We may share information relevant to any request by you for adjustments to the recruitment process as a result of an underlying medical condition or disability with medical/occupational health professionals to enable us to identify what, if any, adjustments are needed in the recruitment process and, if you are successful, once you start work. [*If you do pre-employment medical checks:* We may also share details of disclosed medical conditions and/or answers to pre-employment health questionnaires with medical/occupational health professionals to seek a medical report about you to enable us to assess your fitness for the job and whether any adjustments are needed once you start work.] This information may also be used by the medical/occupational health professionals to carry out assessments required by health and safety legislation. Our ordinary legal grounds for sharing this personal data are that: it is necessary for entry into a contract; and it is in our legitimate interests to consider adjustments to enable Job Applicants to participate fully in the recruitment process. Our additional special category legal ground for sharing this personal data is that it is necessary to comply with our legal obligations/exercise legal rights in the field of employment (obligations not to discriminate, to make reasonable adjustments, to comply with health and safety requirements).

**Legal/professional advisers/insurers**

We share any of your personal data that is relevant, where appropriate, with our legal and other professional advisers and our insurers, in order to obtain legal or other professional advice about matters related to you or in the course of dealing with legal disputes with you or other Job Applicants. Our ordinary legal ground for sharing this personal data is that it is in our legitimate interests to seek advice to clarify our rights/obligations and appropriately defend ourselves from potential claims. Where we share special category personal data, our additional legal grounds for doing so are that: it is necessary to comply with our legal obligations/exercise legal rights in the field of employment; and/or it is necessary to establish, exercise or defend legal claims.

**Home Office**

We may share your right to work documentation with the Home Office, where necessary, to enable us to verify your right to work in the UK. Our legal ground for sharing this personal data is to comply with our legal obligation not to employ someone who does not have the right to work in the UK.

**Your referees**

If you provide us with contact details for professional [and/or character] referees, we may contact them to request information about your previous employment [and their view as to your suitability for the role you have applied for with us]. We will only share with them the details of the job you have applied for and such personal data as necessary to enable them to identify you. [We will only contact your referees once we have made you a conditional offer of employment and you have indicated your acceptance.] Our legal ground for sharing this personal data is that it is in our legitimate interests to verify your suitability for the role and ensure we engage the most suitable candidate.

[*If you use a third party background checking/vetting company*: **Background checking/vetting**

We may share your name, contact details, job applied for, [employment history, qualifications, *insert other ordinary personal data you provide to background checking/vetting company*] with a third party company we engage to conduct background checks on successful Job Applicants. Our legal ground for sharing this personal data is that it is in our legitimate interest to verify your suitability for the role and ensure we engage the most suitable candidate, and to engage appropriate service providers to assist us with this.]

[*If you seek criminal records checks directly from the DBS in respect of jobs on the excepted occupations list:* **Disclosure and Barring Service**

Where you have been offered a job that is on the excepted occupations list under the Rehabilitation of Offenders Act 1974, we may share any of your personal data that is necessary for us to obtain a standard or enhanced criminal records check on you from the Disclosure and Barring Service. Our ordinary legal grounds for doing so are that it is in our legitimate interest to ensure that you are suitable for the role in question and, in certain cases, to comply with a legal obligation. Our additional legal ground for doing so is that it is necessary to comply with a legal obligation/exercise of a legal right in relation to employment and/or that it is necessary for the prevention or detection of unlawful acts (and we process it in accordance with an appropriate policy document).]

[*Insert details of other data sharing, e.g. if you have to disclose applicant data to other regulatory bodies, or if you engage other third party service providers who are in any way involved in processing Job Applicants’ personal data*.]

**[*If you transfer personal data outside the UK:* Transferring personal data outside the UK**

An overseas transfer of personal data takes place when the data is transmitted or sent to, viewed by, accessed by or otherwise used, by a third party in a different country.

Although the UK is no longer a part of the European Economic Area (EEA), the UK Government has recognised the adequacy of data protection provisions in EEA countries. Accordingly, we are able to transfer your personal data to [our parent/group companies] [and ][*name type of recipient, e.g. recruitment agencies*] in the following EEA [country/countries] without restriction: [*name country/countries*].

[*If you transfer personal data outside the EEA:* Data protection law restricts transfers of personal data to countries outside of the EEA because the law in those countries might not provide the same level of protection to personal data as the law in the EEA. To ensure that the level of protection afforded to personal data is not compromised, therefore, we are only able to transfer your personal data outside the EEA if certain conditions are met, as explained below.

[*Transfers to a parent/group company that is based outside the EEA:* As explained above, we share your personal data with [*Name of parent/group company*]. [*Name of parent/group company*] is based outside the EEA, in [*name country*]. [*Either:* There is an adequacy decision [issued by the European Commission and recognised by the UK Government / issued by the UK Government] in respect of [*name country*] meaning that it is deemed to provide an equivalent level of protection for your personal data. *Or:* [*Name of parent/group company*] is based in the USA and has signed up to the UK extension to the EU-US Data Privacy Framework. This is a binding set of commitments that are enforced in the USA by the Federal Trade Commission and which the UK Government has recognised as providing an adequate level of protection for your personal data. *Or:* We have conducted a transfer risk assessment and put in place the following appropriate safeguard[s] to ensure that any personal data transferred to [*name country*] is treated in a way that is consistent with and which respects the EEA and UK laws on data protection and receives an adequate level of protection: [*specify measure, for example, binding corporate rules, the IDTA, or the UK Addendum to the EU standard contractual clauses*]. If you require further information about [this/these] safeguard[s], [you can request it from [*Name, position, email*].]

[*Transfers to other recipients outside the EEA*: We share your personal data with [*name type of recipient, e.g. recruitment agency]*, which is based outside the EEA, in [*name country*]. [*Either:* There is an adequacy decision [issued by the European Commission and recognised by the UK Government / issued by the UK Government] in respect of [*name country*] meaning that it is deemed to provide an equivalent level of protection for your personal data. *Or:* The organisation(s) in the USA to whom we transfer your personal data have signed up to the UK extension to the EU-US Data Privacy Framework. This is a binding set of commitments that are enforced in the USA by the Federal Trade Commission and which the UK Government has recognised as providing an adequate level of protection for your personal data. *Or:* We have conducted a transfer risk assessment and put in place the following appropriate safeguard[s] to ensure that any personal data transferred to [*name country*] is treated in a way that is consistent with and which respects the EEA and UK laws on data protection and receives an adequate level of protection: [*specify measure, for example, the IDTA, or the UK Addendum to the EU standard contractual clauses*]. If you require further information about [this/these] safeguard[s], [you can request it from [*Name, position, email*].]

**Consequences of not providing personal data**

We only ask you to provide personal data that we need to enable us to make a decision about whether or not to offer you a role. If you do not provide particular information to us, then we will have to make a decision on whether or not to offer you a role without that information, which in some cases could result in us deciding not to recruit you. For example, [if we ask you to provide [*an example of previous written work/ a certificate verifying a qualification*] and you do not, we will have to decide whether to recruit you without that information and] if you do not provide us with names of referees or a reference when asked, we will not usually be able to offer you the role. In addition, some of the personal data you provide to us is required by law. For example, if you do not provide us with the documentation we need to check your right to work in the UK, then we cannot by law employ you.

If you choose not to provide us with personal data requested, we will tell/remind you about the implications of any such decision at the relevant time.

**How long will we keep your personal data?**

We will keep your personal data throughout the recruitment process.

If your application is successful and you accept an offer of employment from us, when you start work for us you will be issued with an Employee Privacy Notice which will include information about what personal data we keep from the recruitment process.

If your application is unsuccessful, we will keep your personal data for up to [6 months] from the date we notify you of our decision. If your application is successful, but you decide not to accept our offer, we will keep your personal data for up to [6 months] from the date you inform us of your decision. There may, however, be circumstances in which it is appropriate for us to keep particular items of your personal data for longer. We will base these decisions on relevant circumstances, taking into account the following criteria:

* the amount, nature, and sensitivity of the personal data
* the risk of harm from unauthorised use or disclosure
* the purposes for which we process your personal data and how long we need the particular data to achieve these purposes
* how long the personal data is likely to remain accurate and up to date
* for how long the personal data might be relevant to possible future legal claims
* any applicable legal, accounting, reporting or regulatory requirements that specify how long certain records must be kept

[*If you keep applications on file for longer than the time period specified above:* (Note, we may keep your personal data for longer than [6 months] if you have asked us to consider you for future vacancies – see ‘Will we keep your application on file?’ below).]

Personal data that is held on IT back-up data sets for disaster recovery purposes may also be retained for a longer period. In all cases, we will not keep your personal data for longer than we need it for our legitimate purposes.

**[*If you keep applications on file:* Will we keep your application on file?**

If you are unsuccessful for the role for which you have applied, decline a job offer, or sent us a speculative application, then, if you have consented to us doing so, we will keep your personal data on file to identify if you might be suitable for any other vacancies that may arise in the next [12 months]. We will contact you if we believe this is the case. We will not keep your personal data for this purpose for longer than [12 months].

If during the period that we have your personal data on file, you wish to apply for any particular vacancy that we have open, please do contact us to make us aware of this – particularly if it is not a close match with your previous experience or is in a different area of our business from a vacancy you applied for previously, as we may not otherwise realise that the vacancy would be of interest to you.

When applying for a particular role, there is no obligation for you to consent to us keeping your personal data on file for consideration for other roles if you do not want to. Your application for the particular role you are putting yourself forward for will not be affected.

If you change your mind about us keeping your personal data on file, you have the right to withdraw your consent at any time – see ‘Your rights’, below.]

**References**

If you give us details of referees, we require you to inform them what personal data of theirs you are giving to us. You must also give them our contact details and let them know that they should contact us if they have any queries about how we will use their personal data[, or, if we ask you to do so, you must pass on to them a separate privacy notice in which we explain what we do with their personal data that we receive from you][, although we may also provide them with a specific privacy notice to give them this information].

**[*If you use profiling/solely automated decision-making:* Solely automated decision-making**

Solely automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. [*Provide meaningful details about the logic, significance and consequences of any automated decision-making processes you operate – for example:* For certain roles, we currently require applicants to complete an online psychometric test to determine their suitability to progress further in the recruitment process and be shortlisted for interview. There is a set pass mark for the test and the software automatically rejects applicants who do not meet this pass mark. Applicants who are required to take the test will be given details of who to contact if they are concerned about their score, or wish to query a rejection decision or otherwise obtain human input.]

**Your rights**

You have a number of legal rights relating to your personal data, which are outlined here:

1. **The right to make a subject access request.** This enables you to receive certain information about how we use your data, as well as to receive a copy of the personal data we hold about you.
2. **The right to request that we correct incomplete or inaccurate** personal data that we hold about you.
3. **The right to request that we delete or remove** personal data that we hold about you where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have exercised your right to object to processing (see below).
4. **The right to object to our processing** your personal data where we are relying on our legitimate interest (or those of a third party), where we cannot show a compelling reason to continue the processing
5. **The right to request that we restrict our processing** of your personal data. This enables you to ask us to suspend the processing of personal data about you, for example if you want us to establish its accuracy or the reason for processing it.
6. **The right to withdraw your consent to us using your personal data**. As described above, we do not normally rely on your consent as the legal ground for using your personal data. However, if we *are* relying on your consent as the legal ground for using any of your personal data and you withdraw your consent, you also have the right to request that we delete or remove that data, if we do not have another good reason to continue using it.
7. **The right to request that we transfer** your personal data to another party, in respect of data that you have provided where our legal ground for using the data is that it is necessary for the performance of a contract or that you have consented to us using it (this is known as the right to ‘data portability’).
8. **[*Include if you use profiling/solely automated decision-making:* Rights in relation to solely automated decision-making (including profiling),** including the right to voice your opinion, to obtain human intervention in the decision-making, and to contest the decision.]

If you would like to exercise any of the above rights, please contact [*Name/position/email/address*]. Note that these rights are not absolute and in some circumstances we may be entitled to refuse some or all of your request.

If you have any questions or concerns about how your personal data is being used by us, you can contact our [*if you have a Data Protection Officer*: Data Protection Officer][*if you don’t have a Data Protection Officer*: HR Data Protection Lead/ Data Protection Team] via [*contact details*].

[*If a parent/group company holds/uses any Job Applicant personal data*: If you have any questions or concerns about how your personal data is being used by [*parent/group company*] you can contact their [*if they have a Data Protection Officer*: Data Protection Officer][*if they don’t have a Data Protection Officer*: HR Data Protection Lead/ Data Protection Team] via [*contact details*].

Note too that you have the right to make a complaint at any time to the Information Commissioner’s Office (ICO), the UK supervisory authority for data protection issues. Details of how to contact the ICO can be found on their website: <https://ico.org.uk>