Abaco Job Applicant Privacy Notice

Introduction

This Job Applicant Privacy Notice sets out what personal data we, Abaco Systems Limited ("Abaco", "we" or "us"), 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 or director (together referred to herein as 'Job Applicant' or 'you').

Please note that we will not necessarily hold, use or share *all* 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 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.

This Privacy Notice applies from 25th May 2018, when the General Data Protection Regulation ("GDPR") comes into force. It does not give you any contractual rights. We may update this Privacy Notice at any time.

Applying for a Job with Abaco

Abaco policy is to only process data belonging to Job Applicants where it has been provided through an authorised route. Any data provided via unauthorised routes will not be processes but will be destroyed. The following provides guidance on what is and is not an authorised route:

- **Authorised Routes**
  - Abaco Approved third-party recruitment agencies
  - Abaco internet (www.abacocareers.com)
  - Abaco approved job boards – such as Indeed, Glassdoor or similar
  - Abaco internal job applicants (via the approved process)
  - Abaco employee recommendation (via the approved process)

- **Unauthorised Routes**
  - Unsolicited emails, mail, by hand
  - Personal approaches to Abaco employees
  - Approaches by third-party recruitment agencies not approved by Abaco
  - Any other approach that is not via an Authorised Route

If you supply data to Abaco's third-party recruitment and related service providers, they will have a legal obligation to handle it in compliance with the GDPR. This Notice sets out Abaco's responsibilities when we receive data either directly or via an authorised third party, but does not nullify or replace the responsibilities of third parties.

Who is the data controller?

Abaco Systems Limited, whose registered office and principal place of business is at Tove Valley Business Park, Old Tiffield Road, Towcester, Northamptonshire, NN12 6PF, England, UK is the "controller" for the purposes of data protection law for any Job Applicant data that we receive. This means that Abaco are responsible for deciding how we hold and use personal data about you.

Our Data Protection Officer ("DPO") is 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. They may be contacted in writing at the above address, via email at towcester.gdpr@abaco.com, or by calling +44 (0) 1327 359444.

What is personal data?

Personal data means any information relating to a living individual who can be identified (directly or indirectly) 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 divides personal data into two categories: **ordinary personal data** and **special category data**. Any personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health conditions, sexual life or sexual orientation, or biometric or genetic data that is used to identify an individual is known as **special category** data. (The rest is **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 (if provided), 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
- Other information required to carry out security checks, such as Photo-IDs

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; and
- carry out security checks for the purposes of National Security.

What are our legal grounds for using your ordinary 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 following legal grounds when we process your ordinary personal data:

- We need it to take steps at your request 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, and the obligation we must carry out security vetting to comply with Government security requirements.

- 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 in the section on ordinary personal data, above) 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 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:

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 are 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; and it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.]

Criminal Records Information / DBS checks

We may request criminal records checks from the DBS. We use this information to assess your suitability for the role and verify information provided by you. Our additional legal grounds for using this information is that firstly we have a legal obligation to carry out security vetting in accordance with Government security requirements (i.e. on grounds of National Security and export compliance) and secondly that Abaco has contractual legal requirements that require staff to be security cleared.

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 your application is successful or not.

Some of the personal data about you that we hold and use may come from external sources. For example, a recruitment agency may provide us with your details and/or a shortlist of candidates. If we offer you a role, or an Abaco approved nominated third party working on our behalf will carry out pre-employment checks, such as taking up references from past employers or education providers and checking your qualifications by contacting the awarding body. If we 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. We will also ask candidates to complete a Criminal Records Declaration and we will also seek a criminal record check from the DBS. 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?

Parent / Group Companies

We share any of your personal data that is relevant, where appropriate, with our parent/group company, Abaco Systems, Inc., or other group companies, subsidiaries or branches (“affiliates”) to enable them to input into the recruitment process and approve final recruitment decisions (where applicable). Our legal grounds for doing so are that: it is necessary for entry into a contract, and it is in our legitimate interest to obtain the necessary approvals for our recruitment decisions and comply with the relevant Abaco recruitment policies and procedures. Where sharing takes place with an affiliate based outside the EEA, we ensure that the European Commission has issued a decision confirming that the affiliate’s country provides an equivalent level of protection to personal data, and / or we have put in place the following appropriate measures to ensure that any personal data transferred to them 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 through the use of binding corporate rules and/or clauses in policies used by Abaco and its affiliates. If you require further information about these protective measures, you can request it from the Abaco DPO.

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 related to the recruitment process, to handle baseline security checks and to carry out other administrative recruitment activities. 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 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 due to 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 any pre-employment medical checks are needed, 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 legal grounds for sharing this personal data are that: it is necessary for entry into a contract; it is in our legitimate interests to consider adjustments to enable Job Applicants to participate fully in the recruitment process[and to assess the fitness for work of Job Applicants to whom we have offered jobs; and 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

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

Home Office and other UK Government Departments

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. We may also need to share your information with other UK Government Departments if we need to assess your ability to meet minimum security clearance requirements or process an application for security clearance via the relevant Government agencies. Our legal ground for using this information is that we have a legal obligation to carry out security vetting in accordance with Government security requirements (i.e. on grounds of National Security).

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 proof of qualifications and you do not, we will have to decide whether to recruit you without that information. 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 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, 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 and how long

we keep your personal data whilst you are working for us and after you have left.

If your application is unsuccessful, we will keep your personal data for up to 12 months from the date we notify you of our decision. Note, we may keep your personal data for longer than 12 months if you have asked us to consider you for future vacancies – see 'Will we keep your application on file?' below. 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

In all cases, we will not keep your personal data for longer than we need it for our legitimate purposes.

Will we keep your application on file?

If you are unsuccessful for the role for which you have applied, or you 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 and 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 other vacancies 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.

Solely Automated Decision-Making

Solely automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. Abaco may use automated decision-making to assess things such as eligibility for employment against Abaco minimum security criteria so automated decision-making may be used in the recruitment process to determine such eligibility.

Your Rights

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

- **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 and to check that we are lawfully processing it.
- **The right to request that we correct incomplete or inaccurate** personal data that we hold about you.
- **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).
- **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
- **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.
- **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.
- **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").
- **The right to object to a decision** based on profiling/solely automated decision-making, including the right to voice your opinion, and obtain human intervention in the decision-making.

If you would like to exercise any of the above rights, or if you have any questions or concerns about how your personal data is being used by us, please contact the Abaco DPO in writing. Note that these rights are not absolute and in some circumstances we may be entitled to refuse some or all of your request.

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

---