

Annington Management Limited
Candidate Fair Processing Notice

Last updated: June 2023

Version: V2

Document owner: Data Protection Lead

1. What is this document and why should you read it?

- 1.1 This privacy notice explains how and why Annington Management Limited (also referred to as "Annington", "we", "our" and "us") uses personal data about candidates applying for a job with us (referred to as "you").
- 1.2 This notice does not form part of your future contract of employment or any other contract to provide services.

2. Annington's data protection responsibilities

- 2.1 "Personal data" is any information that relates to an identifiable natural person. Your name, address, contact details, salary details and CV are all examples of your personal data, if they identify you.
- 2.2 The term "process" means any activity relating to personal data, including, by way of example, collection, storage, use, consultation and transmission.
- 2.3 Annington is a "controller" of your personal data. This is a legal term – it means that we make decisions about how and why we process your personal data and, because of this, we are responsible for making sure it is used in accordance with data protection laws.

3. What types of personal data do we collect and where do we get it from?

- 3.1 We collect many different types of personal data about you for lots of reasons. We cannot administer our recruitment/potential employment relationship with you without your personal data. Where we don't need your personal data, we will make this clear.
- 3.2 Further details of the personal data we collect, where we get it from and what we do with it are set out in the table below.
- 3.3 Most personal data we hold about you is collected directly from you throughout the recruitment process with Annington, from when you apply for a job with us, when you complete our new starter forms or correspond with us and in the course of on-boarding you as an employee. We also obtain some personal data from other sources, and create some personal data ourselves.
- 3.4 We also obtain it from other people and organisations, including some public sources, such as publicly available directories and online resources, during recruitment/promotion processes, from recruitment or employment agencies, background check providers (where applicable), former employers, referees and similar, your emergency contacts, your use of Annington provided assets, systems and platforms, training providers, your dependants and beneficiaries, sometimes from the public, and more unusually from the police, government departments or other agencies. You can read more about the sources of personal data in the more detailed information set out in the table below.
- 3.5 If any of the personal information you have given to us changes, such as your contact details, please inform us without delay by contacting dataprotection@annington.co.uk.

Type of personal data	Collected from
a) Contact Information	
<ul style="list-style-type: none">Name(s)TitleAddress(es)Email address(es)Contact details including home and mobile telephone number(s)	<ul style="list-style-type: none">YouRecruitment consultants and agencies
b) Personal Information	
<ul style="list-style-type: none">Date of birthGenderNext of kin or other dependantsMarital or relationship status	<ul style="list-style-type: none">YouRecruitment consultants and agencies

<ul style="list-style-type: none"> • Lifestyle and social circumstances • Emergency contact information 	
c) Identity and Background Information	
<ul style="list-style-type: none"> • Details of education and qualifications and results • Career history, experience and skills • Passport information • Driving licence information • Right to work, residency and/or other visa information (where unrelated to your race or ethnicity) • Curriculum Vitae (CV) or resume and professional profile • Image or photographs • Application form • Evaluative notes and decisions from job interviews • Preferences relating to job location and salary • Conflicts of interests (including where related to family networks) • Results of checks, references and test results (and any associated comments) • Details of referees (title, name, employer/business, contact details), and their opinion of/requested factual details about job applicant 	<ul style="list-style-type: none"> • You • Recruitment consultants and agencies • Your previous employers • Publicly available information from online resources • Referees • Test providers • Providers of background checks and search results
d) Financial Information	
<ul style="list-style-type: none"> • Salary, compensation and other remuneration information • National insurance number and/or other governmental identification numbers 	<ul style="list-style-type: none"> • You • Your previous employer
e) Special Category Personal Data	
<ul style="list-style-type: none"> • Racial or ethnic origin (including your nationality and visa information) • Political opinions • Religious or philosophical beliefs • Trade union membership • Data concerning physical and/or mental health (including occupational health requirements, accident reports, day-to-day health concerns such as diabetes or epilepsy conditions which we should be aware of, dietary requirements, allergies, and reasons for any short term or long term absence) • Sexual orientation • Health and safety and accident records and reports • Information relating to actual or suspected criminal convictions and offences (including DBS checks where mandatory by law) 	<ul style="list-style-type: none"> • You • Your emergency contact(s) • Your use of Annington security control systems when on site • DBS search provider
f) Employment Administration Information	
<ul style="list-style-type: none"> • Recruitment agent and individual contact name and contact information where relevant • Proposed job title • Your working preferences and feedback in relation to Annington and our staff • Your preferences in relation to our use of your personal data • Working time preferences 	<ul style="list-style-type: none"> • You • Recruitment consultants and agencies
g) Security, Location and Access Information when on Site	
<ul style="list-style-type: none"> • Information captured or recorded by electronic card access systems, CCTV and other security control systems 	<ul style="list-style-type: none"> • You • Your use of Annington security control systems

4. What do we do with your personal data, and why?

4.1 We are required by law to always have a permitted reason or justification (called a “lawful basis”) for processing your personal data. The table below sets out the different purposes for which we process your personal data and the relevant lawful basis on which we rely for that processing.

4.2 Please note that where we have indicated in the table below that our processing of your personal data is either:

4.2.1 necessary for us to comply with a legal obligation; or

4.2.2 necessary for us to take steps, at your request, to potentially enter into an employment contract with you,

and you choose not to provide the relevant personal data to us, we may not be able to enter into a contract of employment or engagement with you.

4.3 We process your personal data for particular purposes in connection with your possible future employment or engagement with us, and the management and administration of our business. We are required by law to have a lawful basis (i.e. a reason or justification) for processing your personal data. For some processing activities, we consider that more than one lawful basis may be relevant – depending on the circumstances.

4.4 We may also convert your personal data into statistical or aggregated form to better protect your privacy, or so that you are not identified or identifiable from it. Anonymised data cannot be linked back to you. We

may use it to conduct research and analysis, including to produce statistical research and reports. For example, to help us understand successful recruitment percentages.

Lawful basis and purpose

Consent

Supporting our diversity programmes and staff support networks and initiatives (Note: special category personal data paragraph 5)

Necessary to take steps to enter into an employment contract with you at your request

Making a job offer to you and entering into a contract of employment with you

Communicating with you and providing you with information in connection with your employment or engagement with us from time to time

Necessary to comply with a legal obligation

Complying with right to work compliance obligations

Managing our health and safety compliance obligations

Determining whether any adjustments are necessary to enable you to carry out your role (Note: special category personal data paragraph 5)

Monitoring the security of Annington's physical premises and systems, networks and applications

Complying with equality and non-discrimination compliance obligations

Responding to requests or search warrants or orders from courts, governmental, regulatory and/or enforcement bodies and authorities (Note: special category personal data paragraph 5)

Investigating, evaluating, demonstrating, monitoring, improving, reporting on and meeting Annington's compliance with relevant mandatory legal and regulatory requirements and compliance with binding governance responsibilities (Note: special category personal data paragraph 5)

Responding to employment and industrial relations matters where permitted by applicable law, including criminal investigations, grievances, arbitrations, negotiations, elections and strikes (Note: special category personal data paragraph 5)

Supporting the sale, transfer or merging of part or all of our business or assets, or in connection with the acquisition of another business

Necessary for legitimate interests

To develop and collect feedback on our recruitment activities and employee selection processes to enable us to improve our ability to select the best candidates for positions in the business

Testing candidates, their knowledge, abilities and approach

Administering your application for a job with us and considering your suitability for the relevant role

Conducting background checks, verification and vetting which are not required by law but needed by us to assess your suitability for your role (Note: special category personal data paragraph 5)

Communicating and liaising with you and providing you with information in connection with your employment or engagement with us from time to time

General staff administration, including workforce management and facilities operations

Administering our insurance policies (Note: special category personal data paragraph 5)

Monitoring the security of Annington's physical premises and systems, networks and applications

Supporting the sale, transfer or merging of part or all of our business or assets, or in connection with the acquisition of another business

Investigating, evaluating, demonstrating, monitoring, improving, reporting on and meeting Annington's compliance with relevant legal and regulatory requirements and compliance with best practice and good governance responsibilities (where beyond mandatory legal obligations) (Note: special category personal data paragraph 5)

To obtain legal advice for enforcement and compliance

Benchmarking, research and analysis
Identifying and authenticating candidates and other individuals
Insurance and claims
Responding to requests or non-binding search warrants or orders from courts, governmental, regulatory and/or enforcement bodies and authorities and related parties (Note: special category personal data paragraph 5)
Managing and administering our equal opportunities reporting (Note: special category personal data paragraph 5)
Necessary to protect vital interests
Emergency use, so we can get you the help you need, deal with the emergency services

5. Special category personal data (including criminal data)

5.1 We are required by law to treat certain categories of personal data with even more care than usual. These are called sensitive or special categories of personal data and different lawful bases apply to them. The table below sets out the different purposes for which we process your special category personal data and the relevant lawful basis on which we rely for that processing.

Lawful basis and purpose
<p>Explicit consent</p> <p>Conducting background checks, verification and vetting which are not required by law but needed by us to assess your suitability for your role</p>
<p>Necessary for your/our obligations and rights in the field of employment and social security and social protection law</p> <p>Conducting verification and vetting, including criminal background checks and credit checks where required by law</p> <p>Facilitating the administration of any mandatory healthcare, life assurance/insurance, pensions initiatives and plans that we offer in connection with your employment with us</p> <p>Making reasonable adjustments as needed to help remove barriers faced by you in your role because of any disability you might have</p> <p>Assessing suitability for work, role and demands (duty of care and health and safety obligations)</p> <p>To review your right to work in the UK</p>
<p>It is necessary to protect the vital interests of the data subject or another person you or they are physically or legally incapable of giving consent</p> <p>Contacting the appropriate person in the event of an emergency concerning you</p>
<p>It is necessary for our establishment, exercise or defence of legal claims</p> <p>Identifying, investigating and mitigating suspected misuse of Annington’s assets, systems and platforms</p> <p>Responding to binding and non-binding requests or search warrants or orders from courts, governmental, regulatory and/or enforcement bodies and authorities or sharing information (on a voluntary basis) with the same</p> <p>Complying with disclosure orders arising in civil proceedings</p> <p>Investigating, evaluating, demonstrating, monitoring, improving and reporting on Annington’s compliance with relevant legal and regulatory requirements</p> <p>Responding to employment and industrial relations matters where permitted by applicable law, including criminal investigations, grievances, arbitrations, negotiations, elections and strikes</p>
<p>It is necessary for reasons of substantial public interest</p> <p>Conducting verification and vetting, including criminal background checks and credit checks where required by law</p> <p>Conducting background checks, verification and vetting which are not required by law but needed by us to assess your suitability for your role</p>

Administering our insurance policies

Identifying and authenticating candidates and other individuals

Managing and administering our equal opportunities reporting

It is necessary for preventive or occupational medicine, for the assessment of the working capacity of the employee

Delivering occupational health advice and services to you in relation to your potential role with us

Facilitating the administration of any non-mandatory private healthcare, life assurance/insurance, pensions initiatives and plans that we offer in connection with your employment with us

6. Who do we share your personal data with, and why?

6.1 Sometimes we need to disclose your personal data to other people.

Inside the Annington group

6.2 We are part of a group of companies. Therefore, we will need to share your personal data with other companies in the Annington group (for example, for shared services/division of functions) and our parent company group for key parental decision making and reporting purposes. Where any group companies process your personal data on our behalf (as our processor), we will make sure that steps are taken to protect the confidentiality, security and privacy of your personal data.

Outside the Annington group

6.3 From time to time we may ask third parties to carry out certain business functions for us. These third parties will process your personal data on our behalf (as our processor). We will disclose your personal data to these parties so that they can perform those functions. Before we disclose your personal data to other people, we will make sure that they have appropriate security standards in place to make sure your personal data is protected and we will enter into a written contract imposing appropriate security standards on them. Examples of these third party service providers include service providers and/or sub-contractors, such as our recruitment consultants and agencies, outsourced payroll, HR providers, and our IT systems software and maintenance, back up, and server hosting providers.

6.4 In certain circumstances, we will also disclose your personal data to third parties who will receive it as controllers of your personal data in their own right for the purposes set out above. For example, such disclosure will take place if we work with medical professionals in respect of occupational health or health and safety compliance, or if we work with third parties who carry out background checks and other tests to assess suitability.

6.5 We have set out below a list of the categories of recipients with whom we are likely to share your personal data:

6.5.1 consultants and professional advisors including legal advisors and accountants;

6.5.2 courts, court-appointed persons/entities, receivers and liquidators;

6.5.3 trade associations and professional bodies;

6.5.4 recruitment portal provider;

6.5.5 recruitment agent;

6.5.6 candidate test provider;

6.5.7 insurers; and

6.5.8 governmental departments, statutory and regulatory bodies including the Department for Work & Pensions, Information Commissioner's Office, the police and Her Majesty's Revenue and Customs.

We may also share your personal data with third parties, as directed by you.

7. **Where in the world is your personal data transferred to?**

7.1 Annington is UK based and the majority of our processing of your personal data takes place within the UK. However, in some circumstances your personal data may be transferred to recipients outside the UK (for example, if we use a service provider that is not based in the UK).

7.2 Although data protection laws in some jurisdictions may not provide the same level of protection for your personal data as is provided under the laws in the United Kingdom, we will only transfer your personal data abroad as permitted by law. This includes allowing transfers:

7.2.1 to a country which is recognised as already ensuring an adequate level of protection for personal data;

7.2.2 where appropriate safeguards are put in place with the recipient to protect your personal data, such by use of the official approved standard contractual clauses used for this purpose (called the International Data Transfer Agreement, or the UK Addendum) - please contact Dataprotection@annington.co.uk if you wish to obtain a copy of these;

7.2.3 where the transfer is necessary for a permitted reason specified in data protection law; or

7.2.4 where you consent to the transfer.

8. **How long do we keep your personal data for?**

8.1 We will keep your personal data during the recruitment process and afterwards for as long as is necessary in connection with both our and your legal rights and obligations. If your application is unsuccessful, we will keep your personal data for six months to one year. If your application is successful, we will move relevant details to your employment file and keep them for the period explained in our employee privacy notice. This may mean that we keep some types of personal data for longer than others.

8.2 Any personal data contained in any work related correspondence or records may be retained for longer, dependant on the retention period of the record or file that your personal data is held on.

8.3 Your personal data may be retained following completion of such processing where permitted by law, including:

8.3.1 to comply with any applicable laws or regulations;

8.3.2 to deal with any legal or other type of dispute; and

8.3.3 where we are asked by you or a regulatory authority to keep your personal data for a valid reason.

9. **What are your rights in relation to your personal data and how can you exercise them?**

9.1 You have certain legal rights, which are briefly summarised in the table below, in relation to any personal data about you which we hold.

Your right	What does it mean?	Limitations and conditions of your right
Right of access	Subject to certain conditions, you are entitled to have access to your personal data (this is more commonly known as submitting a "data subject access request").	If possible, you should specify the type of information you would like to see to ensure that our disclosure is meeting your expectations. We must be able to verify your identity. Your request may not impact the rights and freedoms of other people, e.g. privacy and confidentiality rights of other staff.
Right to data portability	Subject to certain conditions, you are entitled to receive the personal data which you have provided to us and which is processed by us by automated means, in a structured, commonly-used machine readable format.	If you exercise this right, you should specify the type of information you would like to receive (and where we should send it) where possible to ensure that our disclosure is meeting your expectations.

		This right only applies if the processing is based on your consent or on our contract with you and when the processing is carried out by automated means (i.e. not for paper records). It covers only the personal data that has been provided to us by you.
Rights in relation to inaccurate personal or incomplete data	You may challenge the accuracy or completeness of your personal data and have it corrected or completed, as applicable. You have a responsibility to help us to keep your personal data accurate and up to date. We encourage you to notify us of any changes regarding your personal data as soon as they occur, including changes to your contact details, telephone number, immigration status.	Please always check first whether there are any available self-help tools to correct the personal data we process about you. This right only applies to your own personal data. When exercising this right, please be as specific as possible.
Right to object to or restrict our data processing	Subject to certain conditions, you have the right to object to or ask us to restrict the processing of your personal data.	This right applies where our processing of your personal data is necessary for our legitimate interests. If you do this, we will need to show either a compelling reason why our processing should continue, which overrides your interests, rights and freedoms or that the processing is necessary for us to establish, exercise or defend a legal claim. You can also object to our processing of your personal data for direct marketing purposes.
Right to erasure	Subject to certain conditions, you are entitled to have your personal data erased (also known as the " <i>right to be forgotten</i> "), e.g. where your personal data is no longer needed for the purposes it was collected for, or where the relevant processing is unlawful.	We may not be in a position to erase your personal data, if for example, we need it to (i) comply with a legal obligation, or (ii) exercise or defend legal claims.
Right to withdrawal of consent	Where our processing of your personal data is based on your consent you have the right to withdraw your consent at any time.	If you withdraw your consent, this will only take effect for future processing.

9.2 If you wish to exercise any of your rights please contact the Data Protection Lead at dataprotection@annington.co.uk in the first instance.

9.3 You also have the right to lodge a complaint with the Information Commissioner's Office, which is the UK data protection regulator. More information can be found on the Information Commissioner's Office website at <https://ico.org.uk/>.

10. Updates to this notice

We may update this notice from time to time to reflect changes to the type of personal data that we process and/or the way in which it is processed. We also encourage you to check this notice on a regular basis.

11. Where can you find out more?

If you want more information about any of the subjects covered in this privacy notice or if you would like to discuss any issues or concerns with us, you can contact us in any of the following ways:

By email at: Dataprotection@annington.co.uk

By telephone at: 020 7960 7500

By post at: The Data Protection Lead, 1 James Street, London, W1U 1DR