

## **Privacy Policy- For Personnel**

In this Privacy Statement the terms, 'we' or 'us' is Axiom DWFM Limited trading as Axiom DWFM.

Your privacy is important to us, and we are committed to keeping your information secure and managing it in accordance with our legal responsibilities under applicable data protection laws. We are registered with the UK Information Commissioner's Office (ICO) as a data controller under registration number ZA199800.

This Privacy Policy sets out the basis upon which we will process personal information we collect from you when you apply for a job with us or through your employment and working arrangements with us as a member of staff, consultant or director.

If you are applying for a job and do not agree with any part of this Privacy Policy, you should not continue with your application.

**Please read this Privacy Policy carefully as it contains important information to help you understand how and why we process any personal information that you give to us.**

### **What Information We Collect**

We process information which:

- You give us when you apply for a job with us.
- We obtain from a recruitment agency when they arrange an application for you.
- We receive from third parties such as credit reference agencies and fraud prevention agencies, former employers etc.
- You give us during your employment relating to your performance, development and training.
- We receive from you or third parties regarding your character and suitability assessment.
- When interacting with us via our website.

### **What personal information we process**

This includes:

- Personal details such as your name, address including address history, telephone number, email address, date of birth
- Identity information and documentation such as National Insurance number, employment history, passport information, Driving Licence,
- Financial Information, including bank details
- Credit history and information relating to you, your partner or anyone else you are financially linked with (we obtain this information from credit reference and fraud agencies or via third party organisations that will engage with you directly to gather your data).
- Information regarding your emergency contacts, qualifications, training and competency records, identifiers assigned to your computer or other internet connected device including your IP addresses, information linked to your mobile telephone number.

We will collect special categories of personal data (e.g. health information regarding a disability, illness or impairment) and criminal and disciplinary records. (See section of Special Categories of Personal Data below for further details).

## Use of Your Information

Your information will be used by us for the following reasons:

PURPOSE	LEGAL BASIS
<b>Recruitment</b>	
To manage job applications and assess candidates for vacancies	<ul style="list-style-type: none"> <li>Legitimate interests for recruitment purposes</li> </ul>
To conduct background checks, including verifying identity and address, validating education, certificates and qualifications, obtaining references, credit reference and criminal records checks and evidence of gaps in employment	<ul style="list-style-type: none"> <li>Legitimate interests to manage and control employee risk</li> </ul>
To obtain evidence of eligibility to work in the UK	<ul style="list-style-type: none"> <li>To comply with legal obligations in the Immigration Act</li> </ul>
To assess the suitability and capability of candidates, including psychometric assessments for certain roles	<ul style="list-style-type: none"> <li>Legitimate interests for recruitment purposes</li> <li>If special categories of personal data are processed- necessary for the purpose of preventative or occupational medicine for the assessment of working capacity.</li> <li></li> </ul>
To document the interview process and assess candidate competence.	<ul style="list-style-type: none"> <li>Legitimate interests for recruitment purposes.</li> <li>If special categories of personal data are processed- necessary for the purpose of carrying out obligations and exercising specific employment rights or for preventative or occupational medicine for the assessment of working capacity.</li> </ul>
<b>During Employment</b>	
To process payroll and pay out of pocket expenses, a record is kept of employees' and consultant bank details, national insurance number and taxation records.	<ul style="list-style-type: none"> <li>Necessary to perform the contract of Employment/ consultancy/ Service Agreement.</li> </ul>

<p>To manage absence, both planned and unplanned and validate fitness and ability to return to work</p>	<ul style="list-style-type: none"> <li>• Legitimate interests for absence management</li> <li>• Necessary for the purpose of carrying out obligations and exercising employment rights or for preventative or occupational medicine for the assessment of working capacity</li> </ul>
<p>For training purposes and to enhance or review performance</p>	<ul style="list-style-type: none"> <li>• Legitimate interests for performance management</li> <li>• To comply with statutory obligations for certain roles and other professional bodies' requirements</li> </ul>
<p>To provide flexible benefits as part of the employee benefits package, if any.</p>	<ul style="list-style-type: none"> <li>• Necessary to perform the contract for optional benefits selected.</li> </ul>
<p>To maintain governance records, including conflicts of interest register, gifts and hospitality log, confidential information lists, staff share dealing disclosures and lists of persons discharging their material responsibility</p>	<ul style="list-style-type: none"> <li>• To comply with corporate governance requirements.</li> </ul>
<p>To update lender panels with information to provide services to clients</p>	<ul style="list-style-type: none"> <li>• Legitimate interests to perform contractual obligations to clients.</li> </ul>
<p>To provide hotel accommodation, company or hire cars</p>	<ul style="list-style-type: none"> <li>• Legitimate interests to facilitate travel for business purposes</li> </ul>

## Security

<p>To monitor access to the office and restricted areas, and to monitor IT systems and applications</p>	<ul style="list-style-type: none"> <li>• Legitimate interests to manage and control information security risk.</li> </ul>
<p>For contacting employees in the event of an emergency or as part of annual testing</p>	<ul style="list-style-type: none"> <li>• To comply with legal obligations</li> <li>• To comply with legal obligations for the prevention of financial crime.</li> <li>• Legitimate interests for business continuity</li> </ul>

### Complying with Legal Obligations

To prevent, investigate and prosecute crime fraud and money laundering

- To comply with legal obligations for the prevention of financial crime and money laundering.

For auditing purposes

- To comply with legal obligations to conduct audits

IF we are obliged to disclose information by reason of any law, regulation or court order.

- 

### Other

To transfer information to any entity which may acquire rights in us

- Legitimate interests for commercial interests

For any other purpose to which you agree

- With your consent

Where we or third parties (see below) process your personal information, it will be processed:

- Because we or they need to do so as a direct consequence of fulfilling your request (for example, to check your identity in order to consider you for a job);
- To comply with applicable laws or regulations, or as permitted by applicable law; or
- On the basis that we or they have a legitimate interest (for example, managing our risk or preventing crime, fraud and money laundering), and in order to protect our business.

### How We Might Share Your Information

The third parties with whom we may need to share personal information to help us provide employment/ consultancy arrangements to you are:

- Providers who need to know the information in order to provide us or you with a service (including BUPA if private medical care is included in your contract of employment, or flexible benefits providers).
- Third party service providers who process information on our behalf to help run some of our internal business operations including background checks, surveys and assessments, training, email distribution, storage of documentation (including for HR and payroll purposes)
- Credit reference agencies to check your identity and obtain credit references.
- Regulators or law enforcement bodies in order to comply with any statutory, regulatory or legal obligation or court order.
- Entities who may or do acquire any rights in us for the purpose of a business sale or reorganisation.

- Lender Panels, regulators and insurers to provide services to clients and meet regulatory obligations.
- Our advisors, for the purpose of assisting us to better manage, support or develop our employees and comply with our legal and regulatory obligations.

These parties may be located in the UK, other countries in the European Economic Area (EEA) or elsewhere in the world. Whenever we or service providers transfer your personal information outside of the EEA, we or they will impose the standard contractual obligations on the recipients of that information to protect your personal information to the standard required in the EEA.

### Retention of your personal information

The personal information that you provide will be retained by us in accordance with applicable laws as follows:

Type of personal information	Retention Period
Recruitment personal data including CVs	<ul style="list-style-type: none"> <li>• Unsuccessful applicants for 6 months from interview</li> <li>• Successful applicants for the relevant period are detailed below as part of the employment/ personnel file.</li> </ul>
Normal personal data	<ul style="list-style-type: none"> <li>• 6 years after the end of employment</li> <li>• 6 years after the end of the consultancy agreement</li> </ul>
Special categorises of personal data: data regarding health	<ul style="list-style-type: none"> <li>• 6 years after the end of employment</li> <li>• 6 years after the end of the consultancy agreement</li> </ul>
Personal financial	<ul style="list-style-type: none"> <li>• Bank Account details are erased 3 months after the end of employment/ termination of consultancy</li> <li>• Records of salary and taxation are retained for 6 years</li> <li>• Records of payment of invoices on consultancy agreements are retained for 6 years.</li> </ul>
Personal location	<ul style="list-style-type: none"> <li>• Attendance records for training 6 years after the end of employment/ termination of consultancy.</li> </ul>

	<ul style="list-style-type: none"><li>• Corporate card statements are retained for 6 years, these may identify location of personnel</li></ul>
Call recordings	<ul style="list-style-type: none"><li>• 1 year</li></ul>
CCTV- digital images	<ul style="list-style-type: none"><li>• 31 days, IT server rooms 90 days</li></ul>

### **Special categories of Personal Data**

Special categories of personal data include information about an individual's health and other categories of personal information which are closely protected (e.g. ethnicity or biometrics). We do not generally process such information, unless you have voluntarily provided that information to us (for example, where you have notified us of a medical issue to allow for reasonable adjustments to be made) or where these are provided or available from a third party or within the public domain as part of initial and ongoing disciplinary and adverse media checks.

### **Email**

Emails sent via the internet can be subject to interception, loss or possible alteration, therefore we cannot guarantee their security. Although we will do our best to protect your personal information, we cannot guarantee the security of your data sent by email and therefore will have no liability to you for any damages or other costs in relation to emails sent by you to us via the internet. If you would like to contact us, please see the section below or use our contact page.

### **Information Security**

We invest appropriate resources to protect your personal information, from loss, misuse, unauthorised access, modification or disclosure. However, no internet-based site can be 100% secure and we cannot be held responsible for unauthorised or unintended access that is beyond our control.

### **Updates**

We will keep this Privacy Policy under review and make updates from time to time.

### **Cookies**

Our website uses cookies (including Google Analytics cookies to obtain an overall view of visitor habits and visitor volumes to our Website).

### **Your Rights**

You have the right to request copies of your personal information we hold. If you think any of the personal information we hold about you is inaccurate, you may request it is corrected or erased. You also have a right, in certain circumstances, to object to our processing of your personal information, to require us to stop processing your personal information and/or to withdraw your agreement to processing based on 'consent'. For further information please write to us at the address below.

**Complaints Process**

If you have a complaint about how we have handled your personal information please contact us using the details below and we will investigate your complaint. You also have the right to complain to the Information Commissioner's Office – ([www.ico.org.uk](http://www.ico.org.uk)).

**Contact Us**

You can contact us by writing to us at:

Axiom DWFM Limited

101 Wigmore Street, London, W1U 1FA.

Data Protection Manager: Pragnesh Modhwadia

Telephone queries can be made to 020 8951 6989

Email requests can be made to [pm@axiomdwfm.com](mailto:pm@axiomdwfm.com)

Signed

Full name .....

Date .....