Job Candidate Privacy Notice

1. Introduction

1.1. Who are we, and what is the purpose of this notice?

Dragonfly Eye Ltd, its branches and subsidiaries ("we", "us", "our", "Dragonfly") located in the United Kingdom, Singapore and the United States, provides a private intelligence service to decision makers in the world's leading organisations. We are committed to protecting your privacy and handling your personal data in accordance with Data Protection Laws.

Dragonfly is a "data controller" of personal data processed as part of our recruitment process. This means that we are responsible for deciding how we hold and use personal information about you. You are being sent a copy of this privacy notice because you are applying to work with us (whether as an employee, worker or contractor).

Data Protection Law means the Data Protection Act 2018, the UK General Data Protection Regulation (UK GDPR), Privacy and Electronic Communications Regulations and any other applicable local privacy laws in jurisdictions we operate in, as any of the same may be amended, superseded or replaced from time to time.

1.2. Scope

This notice applies to candidates for vacant roles that we advertise either via our website or through a recruitment agency and any speculative job applications that you make to Dragonfly ("candidates").

If we offer or have offered you a position, then our 'Employee Privacy Notice' outlines how we will use your data in the course of the onboarding process and once you have joined us. The Employee Privacy Notice will be made available to you in the event that we make you an offer of employment.

1.3. Purpose

The purpose of this notice is to make you aware of the personal data we collect, how we use it, with whom we share it and how we protect it.

This notice makes you aware of how and why your personal data will be used, namely for the purposes of the recruitment exercise, and how long it will usually be retained for. It provides you with certain information that must be provided under Data Protection Law.

2. Policy

2.1. General principles

We will comply with the UK GDPR principles, which means that your personal data will be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Adequate, relevant and limited to what is necessary to achieve those purposes.
- Kept accurate and up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept securely.

Which of your personal data do we collect and how do we collect it?

Like all prospective employers, we may collect and process personal data that you provide to us in the course of the recruitment process.

The personal data we collect from you will vary from time-to-time as required for us to manage your progress within the recruitment process and to meet legal and regulatory requirements. Personal data we collect about you may include for example: contact details; information on academic and professional qualifications and memberships; historic employment information; correspondence with or about you; records of assessments that we may ask you to participate in and any information you provide to us during an interview relevant to assessing your suitability for the role.

The lawful basis we rely on for processing your personal data is article 6(1)(b) of the UK GDPR, which relates to processing necessary to perform a contract or to take steps at your request, before entering a contract.

Where your application has been unsuccessful, we may wish to keep your personal data for a longer period and add it to our talent pool to contact you about future vacancies. We will only do so if you give us your consent. You can withdraw your consent at any time.

We will process your personal data only for the purposes set out in this section.

If we are required to process your personal data for any purpose other than those included in this section, we will notify you of this before doing so.

2.2. Handling

How do we use your personal data?

We will use the personal data we collect about you to:

- Assess your skills, qualifications, and suitability for various roles in our business
- Carry out background and reference checks, where applicable
- Communicate with you about the recruitment process
- Keep records related to our hiring processes
- Comply with legal or regulatory requirements
- Decide whether to enter into a contract of employment with you

In summary, we generally use your personal data in order to evaluate your suitability for a role with Dragonfly, to manage our relationship with you as your potential employer and to comply with our legal obligations.

How do we use your particularly sensitive personal data?

We do not request particularly sensitive personal data from candidates. However, if you provide us with any information about reasonable adjustments you require under the Equality Act 2010 the lawful basis we rely on for processing this information is article 6(1)(c) of the GDPR to comply with our legal obligations under the Act and relates to our obligations in employment and the safeguarding of your fundamental rights.

In more detail, we use your personal data for the following purposes on the following legal bases:

Purpose for processing	Categories of personal data processed	Collection method and legal bases
Evaluation of speculative job applications and application responses Including as required to establish whether or not you are a suitable candidate for a role, your right to work in the country and whether to progress your application in the recruitment process.	• Contact details • Qualification details and employment history • Correspondence • Assessment results and responses • Documents confirming your right to work as applicable	Method of collection: We collect this data if you respond to a job opening during the recruitment process or send us a speculative job application. Legal basis for processing: we process your personal data because it is necessary to take steps at your request, before entering a contract.
Testing and assessments Including as required sharing your personal data with our appointed third-party provider(s) of aptitude testing (see below at “How do we share your personal data?”)	• Contact details • Assessment results and responses	Method of collection: We collect this data during the recruitment process. Legal basis for processing: we process your personal data because it is necessary to take steps at your request, before entering a contract.
Application management and administration Including, contacting you regarding your application, arranging interviews and other meetings with you, answering any questions you might have about the recruitment process and adding your details into our HR recruitment system.	• Contact details • Qualification details and employment history • Correspondence	Method of collection: We collect this data when we receive speculative interest from you in vacancies, when evaluating job applications received from you for suitability for roles and when communicating with you regarding the recruitment process. Legal basis for processing: we process your personal data because it is necessary to take steps at your request, before entering a contract.

Legal and regulatory compliance We may need to retain certain data about you in order for us to defend ourselves against any future legal claims that may be brought. We may also be required to share your information with the police	• Contact details • Qualification details and employment history • Correspondence • Assessment results and responses • Documents confirming your right to work as applicable	Method of collection: We collect this data during the recruitment process. Legal basis for processing: It is our legitimate business interest to defend ourselves against any future claims that may be brought against us. We have a legal obligation to share your personal data with security services for law enforcement purposes.
Contact you about future opportunities In the event that you are not successful in your application for a role with us, we will keep your details on record in case there are any other opportunities that arise within our company that we feel you may be suited to.	• Contact details • Qualification details and employment history	Method of collection: We collect this data during the recruitment process. Legal basis for processing: We obtain your consent to add your personal data to our talent pool.

What happens if you fail to provide personal data?

If you fail to provide information when requested, which is necessary for us to consider your application (such as evidence of qualifications or work history), we will not be able to process your application successfully. For example, if we require a credit check or references for a role and you fail to provide us with relevant details, we will not be able to take your application further.

How do we share your personal data?

We may share your personal data with:

- other companies within our group
- selected third-party service providers, where necessary, to provide us or you with services, which may include:

- Credence – employment screening company;
- any relevant recruitment agent who you have been in touch with about the role that you are applying for;
- The Risk Advisory Group Ltd - which provides support services to Dragonfly, including for recruitment, selection and onboarding purposes;
- Sage People to host your data and assist us with administering the recruitment process.

We only transfer your personal data to third parties, including those outside of the jurisdiction where you are located (see below at "Do we transfer your personal data internationally?"), if we are satisfied they take appropriate measures to protect it and any necessary contractual documentation is in place to ensure the integrity and security of the data as required by law.

Where we are required to disclose your personal data to law enforcement agencies and regulatory bodies to comply with our legal and regulatory obligations, we may be unable to inform you of such disclosures.

Do we transfer your personal data internationally?

As a multinational organisation, and in line with the global nature of our services, we may transfer personal data internationally. Accordingly, your personal data may be transferred globally (if your data is collected within the United Kingdom, this means that your data may be transferred outside it, if your data is collected outside of the United Kingdom, this means that your data may be transferred into it).
In respect of internal transfers within the Dragonfly group, we have entered into an intra-group agreement, using the Standard Contractual Clauses, to ensure your data receives an adequate level of protection.

Where we transfer your personal data externally to countries where there is no adequacy decision by the Information Commissioner in respect of that country, we will put in place appropriate measures to ensure that your personal data receives an adequate level of protection, such as standard contractual clauses that have been approved by the Information Commissioner's Office.

What rights do you have over your personal data?

You may have some or all of the following rights under applicable law in respect of the personal data that we hold about you:

- request us to give you access to it
- request us to rectify it, update it
- request us to erase it, in certain circumstances
- request us to restrict our using it, in certain circumstances
- object to our using it, in certain circumstances
- withdraw your consent to our using it
- request us to transmit your personal data to you or to another party (data portability), in certain circumstances; and
- lodge a complaint with the supervisory authority in your country (if there is one)

To the extent that we rely upon your consent or explicit consent as the legal basis under which we process your personal data, you are entitled to withdraw your consent at any time.

You are able to exercise these rights by contacting us using the details set out below at "Who should you contact with questions?".

What security arrangements do we have in place to protect your personal data?

We implement appropriate technical and organisational measures to protect personal data that we hold from unauthorised disclosure, use, alteration or destruction. Dragonfly has in place various safeguards to protect all data, including your personal data. This includes the following measures in relation to:

- unauthorised disclosure or use: access to candidate and employee personal data is given on a need to know basis, and is authorised by senior management. Segregation of duties is in place to restrict access. The systems holding data are secured from unauthorised access with logins traceable to individuals and multi-factor authentication. Data is marked using a document classification scheme to define the permissible level of sharing and the required security restrictions that need to be applied.
- alteration or destruction: all systems have detailed logging in place, data is being backed up to the alternative location where it is stored encrypted.

How long will your data be retained for?

The period for which we may retain data about you will depend on the purposes for which the data was collected, whether you have requested the deletion of the data, and whether any legal obligations require the retention of the data (for example, for regulatory compliance).

If we offer you employment at Dragonfly and you accept, then the retention periods that apply to your data are set out in the employment privacy notice that we will provide to you upon making you an offer.

Otherwise, we will only retain any assessment results and responses until the recruitment process has ended. Your contact information, qualification details and employment history are generally only kept on record for one year following the end of the recruitment process if you have no ongoing job applications or have not been added to our talent pool. Where you have consented to be added to our talent pool, your personal data will be held for two years following the end of the recruitment process.

Employment screening information is kept by the HR department for the first 6 months of employment and it is then securely destroyed.

3. Implementation

This notice is available to all candidates via the careers page on the company's website.

We keep our privacy notice under regular review to make sure it is up to date and accurate. The new modified or amended privacy notice will apply from that revision date. Therefore, we encourage you to review the careers page periodically to view the most up to date version of the privacy notice and be informed about how we are processing your personal data.

This privacy notice was last reviewed in September 2022.

This privacy notice does not form part of your contract of employment, and we may update it from time to time.

This privacy notice overrides any notice previously communicated to you.

4. Governance

This policy is owned by HR and overseen by the Data Protection Officer to ensure compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal information, please contact HR or the Data Protection Officer.

Who should you contact with questions?

If you have any questions or concerns about our handling of your personal data or this privacy notice, please contact the Head of Human Resources at hr@dragonflyintelligence.com or on +44 20 3653 0010 or the Data Protection Officer at dpo@dragonflyintelligence.com.

You have a right to contact the Information Commissioner's Office, the UK supervisory authority for data protection issues (www.ico.org.uk/concerns)with any questions or concerns in relation to how your personal data is processed by us. We request that you raise these with us in the first instance by contacting our DPO using the email address above.