



Version	1.02
Document Reference	CYJ-0093
Classification	Public
Effective Date	19/02/2025
Last Review Date	24/02/2026
Next Review Date	24/02/2027
Document Owner	Chief Compliance Officer
Document Approver	ISMF (Information Security Management Forum)
Document Summary	This policy details how we store, process and handle personal information of candidates applying for positions at CYJAX.

This Privacy Notice (“Notice”) describes how CYJAX collects, uses, maintains and discloses information from our website and platforms. If you have any comments or concerns about this Notice, please contact us using the details at the end of it.

## Candidates’ privacy notice

CYJAX respects your privacy and is committed to protecting your personal data. When you apply for a position at CYJAX we process your data and are the data controller. This means that we are responsible for deciding how we hold and use your personal data.

This notice explains how we obtain and manage your data during the recruitment and selection process whether as an employee, consultant or contractor.

### 1 Collection of personal data and use

In connection with your application, most of the information will be provided by you or someone on your behalf with your knowledge, such as a recruitment agent or a referee. The information we will collect, use and store will usually include:

- Personal Identification Information: Name, contact details (email address, phone number), and address.
- Job Application Information: CV/resume, cover letter, job application form, and references.
- Recruitment and Interview Data: Notes from interviews, feedback, test results, and assessment data.
- Eligibility and Qualifications: Proof of qualifications, certifications, work history, educational background, and employment references. We also collect and process documentation required to verify your legal eligibility to work, including passports, visas, biometric residence permits, or other immigration-related evidence. This information is necessary for us to comply with employment and immigration legislation and to complete mandatory pre-employment verification checks.
- Sensitive Data (if applicable): In certain cases, we may collect sensitive data such as health-related information, disability status, or equal opportunity monitoring information (e.g., race, ethnicity, gender). This will be collected only with your explicit consent, where necessary, and will be processed in accordance with applicable laws.

### 2 How we use your personal data

- To assess your suitability for a position: We will use your CV, application form, and other information to assess your qualifications, skills, and experience for the role you have applied for.
- To communicate with you: We will use your contact details to arrange interviews, send test results, request additional information, or inform you about the status of your application.
- To evaluate your skills: If applicable, we may request you to complete skills assessments or tests relevant to the role.
- To comply with legal obligations: We may use your data to ensure compliance with employment laws, equal opportunity regulations, or other legal requirements.
- To verify your information: We may use your data to verify your employment history, qualifications, and other relevant background checks (e.g., criminal record checks, reference checks).

### 3 Lawful basis for processing personal data

We process your personal data based on the following lawful grounds:

- Contractual Necessity: Processing is necessary to take steps before entering an employment contract with you.
- Legitimate Interests: We process personal data based on our legitimate interests in evaluating candidates and ensuring the recruitment process runs efficiently.
- Consent: In certain cases, we may rely on your explicit consent to process sensitive data, such as health information or other special categories of data.
- Legal Obligations: We may process personal data to comply with legal obligations, such as equal opportunity monitoring or background checks.

### 3.1 Sensitive personal data

We will use your sensitive personal data only insofar as we are permitted by law to do so:

- We will use data about your disability status to consider whether we need to provide appropriate adjustments during the recruitment process, for example whether adjustments need to be made during a test or interview.
- We will use data about your nationality or ethnicity to assess whether a work permit and a visa will be necessary for the role.

### 3.2 If you fail to provide personal data

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

## 4 Retention of data

We will retain your personal data for a period of 6 months (if you are unsuccessful). If you are successful, we will retain your information in line with our retention policy, which will be accessible in the CYJAX Intranet site.

We retain your personal data for that period so that we can show, in the event of a legal claim, that we have not discriminated against candidates on prohibited grounds and that we have conducted the recruitment exercise in a fair and transparent way. We further retain such personal data in case a similar role becomes vacant for which you will be a fitting candidate. After this period, we will securely destroy your personal data in accordance with our data retention policy.

## 5 Security

CYJAX is dedicated to ensuring that all information is protected against unauthorised access, processed appropriately, and held securely in accordance with the UK and EU General Data Protection Regulation (GDPR) and Data Protection Act 2018.

Our ISMS (information security management system) is certified to ISO/IEC 27001, demonstrating that we have the appropriate Framework in place to ensure that all our information assets and networks are secure.

All data is encrypted both in transit, end-to-end and at rest using AES-256.

## 6 Storage and transfer

We will make every practical effort to store and process your information in the country in which it was submitted. However, some of our third-party suppliers may be based outside the UK and European Economic Area (EEA), so there may be instances when data is stored and transferred outside the UK or EEA. In the eventuality that data is transferred outside these areas, we have the following safeguards in place.:

- The country or relevant territory has an adequate level of protection as recognised by the GDPR.
- Specific contracts approved by the appropriate Commission which give your personal information the same protection it has as if it stayed in the UK or EEA along with effective data controls.
- The third-party supplier has met our data security standards and is compliant with our information management security framework.
- All data is encrypted both in transit, end-to-end and at rest.
- Data is stored within defined retention periods and is regularly reviewed.

**Transfer Risk Assessments (TRAs):** Where personal data is transferred outside the UK or EEA to a country that is not covered by an adequacy decision, CYJAX conducts Transfer Risk Assessments to evaluate whether the destination jurisdiction provides protection essentially equivalent to that required under the UK GDPR. These assessments ensure that any international transfer is subject to appropriate safeguards and that the security and confidentiality of your personal data are maintained.

## 7 Sharing

We will only share your data internally (with staff who need the information to assess your application) and with third parties for the purposes of progressing your application, confirming your suitability for employment following a job offer and preparing for the commencement of your engagement with us. The third parties may include your recruitment agent or any job advertising platform through which you apply to us, and any party necessary for pre-employment screening.

CYJAX or its service providers share your personal data with third parties when:

- required by law.
- requested by a regulator.
- necessary to manage its working relationship with you/process your application.
- it is in the public interest to do so.
- necessary for fraud and data error investigations.

This may involve sharing special category personal data if you chose to provide it. The third parties include the following service providers:

Third party	Purpose
Adobe	Contract e-signing
M365	Document storage and email
Verifile	Right to work and employment screening

**Additional Third-Party Processors:** In addition to the service providers listed below, CYJAX may engage other third-party organisations that support our recruitment and selection processes, such as applicant tracking system providers, online skills testing platforms, background screening partners, and human resources information systems. All such third parties are contractually bound to process personal data only in accordance with our instructions and to implement appropriate security and confidentiality measures.

All our third-party service providers are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

## 8 Your rights in relation to personal data

Under data protection laws in the European Union and the UK, you have certain rights in relation to your personal information. You have the right:

- to be informed about the collection and the use of your personal data.
- to access personal data and supplementary information.
- to have inaccurate personal data rectified or completed if it is incomplete.
- to erasure (to be forgotten) in certain circumstances.
- to restrict processing in certain circumstances.
- to data portability, which allows the data subject to obtain and reuse their personal data for their own purposes across different services.
- to cease/object to processing in certain circumstances.
- rights in relation to automated decision making and profiling.
- to complain to the Information Commissioner.
- Withdraw your consent at any time.

A full list of your rights under the UK General Data Protection Regulation (GDPR) is available on the Information Commissioner's Office (ICO) website.

We will handle all requests in accordance with applicable law. However, depending on the right you wish to exercise, and the nature of the personal information involved, there may be legal reasons why we cannot grant your request. If this is the case, we will write to you to explain the reasons why.

## 9 Accessing, rectifying, restricting, objecting or erasure of your personal information.

To exercise your right to access, rectify, restrict, object to processing of, or erase the personal information CYJAX holds about you, please contact our Data Privacy Manager at [privacy\[at\]cyjax.com](mailto:privacy[at]cyjax.com) or, if you are based in the EU or our EU Representative (details below).

Requests will be acknowledged within three working days, with the final response and disclosure of information (subject to exemptions) within 30 calendar days.

A 'cease processing request' from an individual will be acknowledged immediately with an automatic email response stating that CYJAX intends to comply with the request.

For information on the Privacy and Electronic Communications (EC Directive) Regulations 2003, UK General Data Protection Regulation (GDPR), Data Protection Act 2018 and the Information Commissioner's Office, please follow this link: <https://ico.org.uk/>.

CYJAX is registered with the United Kingdom Information Commissioner's Office (ICO) under reference ZA053004, as required by UK (United Kingdom) legislation.

### 9.1 EU (European Union) Representative

As we do not have an establishment in the European Union ("EU"), we have appointed a representative based in Ireland, who you may contact if you are located in the EU to raise any issues or queries you may have relating to our processing of your Personal Data and/or this Privacy Notice. Our EU representative is Data Protection Limited, located at 2 Pembroke House, 28-32 Upper Pembroke Street, Dublin, Ireland D02 EK84. Our EU representative can be contacted directly on 00 353 1 447 0402 or at [cyjax@willansdps.com](mailto:cyjax@willansdps.com).

## 10 How to raise a Complaint

If you have concerns about how we collect or use your personal data, we encourage you to contact us first. We are committed to resolving privacy complaints quickly and fairly.

### Step 1: Contact Us

Email: [privacy\[at\]cyjax.com](mailto:privacy[at]cyjax.com)

Post: Data Protection Officer, First Floor, 1 Des Roches Square, Witan Way, Witney, OXON OX28 4BE

Please include: Your full name and contact information, a summary of your concern and any relevant dates or evidence.

### Step 2: Our Response

We will acknowledge your complaint within 30 days. You will receive a full response as soon as possible (typically within 45 days).

### Step 3: If You're Not Satisfied

If you are not happy with our response, you may escalate the matter to the Information Commission (ICO): <https://ico.org.uk/make-a-complaint/>

## Document History

Revision Version	Revision Date	Description of Revision	Revision Author(s)
1.02	24/02/2026	Reviewed. Updated to include info on TRA and further info of RTW	Louise Cook
1.01	18/9/2025	Added in information about how to raise a complaint	Louise Cook
1.00	19/02/2025	Separated from website privacy notice.	Louise Cook