

CANDIDATE PRIVACY NOTICE

1. INTRODUCTION

At OneAdvanced, we are committed to protecting your personal data and privacy. This **Candidate Privacy Notice** explains how OneAdvanced processes your personal data when you apply for a position with us. We are committed to protecting your privacy, rights, and freedoms regarding your personal data in accordance with the UK GDPR, Data Protection Act 2018 (DPA 2018), Data Use and Access Act 2025 (DUAA 2025) and other applicable data protection laws (Data Protection Legislation).

This notice describes how we collect, store, use, and share personal information, and explains your rights in relation to the personal information we hold about you.

This notice applies to all candidates globally, including those applying for permanent, fixed-term, contractor, intern, trainee, and graduate positions within the OneAdvanced Group. It covers the collection and use of your information during the recruitment process only. Once you become an employee, our Colleague Privacy Notice will apply, and you will be provided with access to it.

This notice is subject to regular review and update to ensure continued compliance with evolving data protection requirements and organisational changes.

2. WHO WE ARE

When we say "we" "us" or "OA" in this Privacy Notice, we're referring to **OneAdvanced Limited**, a company registered in England and Wales (registration number 05965280) with its registered office at The Mailbox Level 3, 101 Wharfside Street, Birmingham, United Kingdom, B1 1RF.

Please note that other entities within OA may also act as employers and therefore process your personal data as Data Controllers. Please refer to your contract to identify the specific entity applicable to your employment. For a full list of OneAdvanced legal entities, please visit our website [here](#).

3. WHAT INFORMATION WE COLLECT ABOUT YOU

We collect your information throughout the recruitment process. The specific types of personal data we collect vary by country due to different legal frameworks. The general categories of personal data we collect include:

- **Identification and Contact Details:** Your name, address, and contact details, including email address and mobile numbers. In some countries, we also collect marital status. In the US, we may collect information about Latino background or veteran status for reporting purposes.
- **Education and Training:** Training records and professional certifications relevant to the role you have applied for.
- **Employment Information:** Employment history, references, CVs, screening outcomes, desired start dates, department preferences, line manager preferences, salary expectations, and benefits information.
- **Government Identification Data:** Passport details, national identifier information (such as National Insurance Number in the UK), driving licences, or other permits as required for the role.

- **Diversity Information:** Ethnic origin, religious or similar beliefs, sexual orientation, and details of any disabilities. We only collect this information where we have a lawful basis and appropriate condition to do so, and provision is always voluntary.
- **Referee Information:** Contact details and information about individuals who provide references for you. We use this information solely to obtain references and retain copies on your file if you are successful in your application.
- **Health Information:** Any health information you provide to enable us to make reasonable adjustments for interviews, assessments, or potential employment. We implement specific safeguards for health information processing, including restricted access controls, enhanced security measures, and clear consent mechanisms where required.
- **Remuneration Information:** Details about your current remuneration package and future expectations regarding salary, benefits, and pensions.
- **Social Media Information:** Links to your professional social media profiles and publicly available information from professional networking sites.
- **Images and Recordings:** As part of our recruitment process, particularly for remote interviews, virtual assessment centres, or specific skill assessments, we may collect photos, video recordings, and voice recordings, including:
 - Video interviews conducted via platforms such as Microsoft Teams, Zoom, or dedicated recruitment tools.
 - Virtual assessment centre participation recordings.
 - Voice recordings for language proficiency or communication assessments and
 - Identity verification images for online assessment integrity.

4. WHERE WE COLLECT YOUR PERSONAL INFORMATION FROM

We collect personal information directly from you and from the following sources:

- **Recruitment and Employment Agencies:** Those with whom we have established contractual arrangements.
- **Professional Networking Sites:** Such as LinkedIn, both when you apply via these platforms or when we proactively search for candidates.
- **Online Platforms:** Recruitment websites, internet searches, CV databases, and job boards.
- **Career Events and Networks:** Information collected at career fairs, networking events, and professional gatherings.
- **Employee Referrals:** Information provided by our current employees who refer candidates.
- **Background Screening Providers:** These services may involve requesting data from law enforcement agencies, previous employers, and other relevant third parties.
- **Government Departments:** Such as driving licence authorities to verify eligibility for roles requiring business driving.

Where consent is required by law, we will obtain your explicit consent before collecting such information. Where consent is not required, we will inform you in advance of collection.

5. LAWFUL BASIS FOR PROCESSING

5.1 UK Candidates

For candidates based in the UK, we rely on the following lawful bases under Article 6 of the UK GDPR:

- **Legitimate Interests** (Article 6(1)(f)): For recruitment processing, assessment of suitability, communication about applications, and business analysis. We have conducted a Legitimate Interests Assessment confirming that our interests in effective recruitment do not override your fundamental rights and freedoms. A summary of the LIA key findings can be requested from the Talent Acquisition Team.
- **Legal Obligation** (Article 6(1)(c)): For right to work checks, diversity monitoring required by law, and compliance with employment legislation.
- **Consent** (Article 6(1)(a)): Where explicitly obtained for specific processing activities such as background checks. These include:
 - Employment checks.
 - Criminal record search.
 - Driving records check (where required).
 - Adverse financial history checks.
 - Adverse media checks.
 - Right to Work checks.
 - Extra jurisdiction checks.

5.2 Special Category Data

Where we process special category data (including health information, diversity data, or other sensitive personal data as required), we rely on the following conditions under Article 9 of the UK GDPR:

- **Explicit Consent** (Article 9(2)(a)): For voluntary diversity monitoring and health information provided for reasonable adjustments. We ensure explicit consent is obtained through clear, separate consent mechanisms that allow withdrawal at any time without affecting your application.
- **Employment, Social Security and Social Protection** (Article 9(2)(b)) with Schedule 1, Part 1, Paragraph 1 of the DPA 2018: For processing necessary for employment purposes.
- **Substantial Public Interest** (Article 9(2)(g)) with Schedule 1, Part 2 conditions of the DPA 2018: Including statutory and government purposes and equality of opportunity monitoring where required by law.

5.3 Other Jurisdictions

The lawful basis for processing your personal data in other jurisdictions depends on your location and the applicable data protection laws:

Country	Lawful Basis
Ireland	Legitimate interests for recruitment purposes; consent for special category data; legal obligation where applicable.
Australia	No specific lawful basis required for non-sensitive information; consent required for sensitive information.
India	Lawful basis required for processing; consent and lawful purpose required for sensitive personal data.

Recognised Legitimate Interests: Under the Data (Use and Access) Act 2025, we may process your personal data for recognised legitimate interests including:

- Crime prevention and detection relevant to employment screening.
- Safeguarding vulnerable individuals in roles involving vulnerable populations and
- Emergency response capabilities for business continuity roles.

6. HOW WE USE YOUR INFORMATION

We use your personal information for the following purposes:

- **Recruitment Processing:** To assess your suitability for the role, conduct interviews, and make employment decisions.
- **Communication:** To communicate with you about your application, arrange interviews, and provide updates on your application status.
- **Verification:** To verify your identity, qualifications, employment history, and eligibility to work.
- **Reasonable Adjustments:** To make reasonable adjustments for interviews, assessments, or potential employment based on health information you provide.
- **Legal Compliance:** To comply with legal obligations including diversity monitoring, health and safety requirements, and employment law obligations.
- **Business Analysis:** To analyse recruitment effectiveness and improve our recruitment processes on an anonymised basis.

6.1 Purpose Limitation and New Processing Activities

If we wish to use your personal data for a new purpose not originally disclosed to you, we will:

- Conduct a compatibility assessment to ensure the new purpose is compatible with our original collection purposes.
- Where applicable, obtain your consent for the new processing.
- Update this Privacy Notice to reflect the new purpose.

- Notify you directly of the new purpose before commencing any new processing.
- Provide information about the retention period for the new purpose and
- Inform you of your rights regarding the new processing.

7. DATA SHARING AND INTERNATIONAL TRANSFERS

We may share your personal data with:

- Other entities within the OneAdvanced Group.
- Recruitment agencies and employment service providers.
- Background screening providers.
- Professional referees and previous employers.
- Assessment and testing service providers and
- IT service providers supporting our recruitment systems.

7.1 International Transfers:

We operate globally and may transfer your personal data internationally within our OA entities and to third-party service providers. We ensure that international transfers comply with UK GDPR requirements through:

- **Adequacy Decisions:** Transfers to countries recognised by the UK as providing adequate protection (including EU Member States under the EU Adequacy Decision) **or**
- **Standard Contractual Clauses (SCCs) or International Data Transfer Agreements (IDTAs):** Contractual protections approved by the EU and UK authorities for transfers to countries without adequacy decisions **or**
- **Additional Safeguards:** Technical and organisational measures to protect your data during international transfers.

8. DATA RETENTION

We retain your personal data for the following periods:

- **Successful Candidates:** Personal data collected during recruitment is transferred to our employee records and retained in accordance with our Employee Privacy Notice and UK legislative data retention requirements for personnel records.
- **Unsuccessful Candidates:** Personal data is retained for 12 months from the date of our final decision to enable us to respond to queries and consider you for future suitable roles.
- **Withdrawn Applications:** Where you withdraw your application, we retain basic contact details for 6 months and delete other personal data immediately.
- **Legal Requirements:** We may retain personal data for longer periods where required by law, such as for diversity monitoring reporting or to defend legal claims.
- **Anonymised Data:** We may retain anonymised statistical information indefinitely for business analysis purposes.

9. YOUR RIGHTS

Subject to applicable local laws, you have the following rights regarding your personal data:

- **Right of Access:** Request confirmation of what information we hold about you and how it is processed by emailing dataprotection@oneadvanced.com.
- **Right to Rectification:** Update your personal information by submitting requests via the Digital Workspace or by emailing hr@oneadvanced.com if you no longer work for the organisation.
- **Right to be Informed:** This Privacy Notice provides information about what personal data we collect and how it is used and is regularly updated to reflect changes in our processing activities.
- **Right to Object:** Object to processing of your personal data where we rely on legitimate interests as the lawful basis.
- **Right to Erasure (Right to be Forgotten):** In certain circumstances, request deletion of your personal data via the Digital Workspace or hr@oneadvanced.com.
- **Right to Restrict Processing:** In certain circumstances, request restriction of your personal data processing.
- **Data Portability:** Request your data in a machine-readable format for transmission to another Data Controller.
- **Rights regarding Automated Decision-Making:** No automated decision making processes are currently being used.

10. SUBJECT ACCESS REQUESTS

- **Request Process:** You can submit subject access requests via dataprotection@oneadvanced.com
- **Response Timeframe:** We will respond to your request within one month of receipt, or within an additional two months for complex requests, as permitted under the UK GDPR.
- **Additional Information Requirements:** We may pause the response timeframe if we require additional information from you to locate or verify your data. The response time will resume once we receive the necessary information from you.
- **Reasonable and Proportionate Searches:** We will conduct reasonable and proportionate searches to locate your personal data and are not required to conduct excessive or disproportionate searches.

11. COOKIES AND TRACKING TECHNOLOGIES

Our recruitment platforms and website use cookies and similar technologies for:

- Essential website functionality and security.
- Statistical analysis to improve our services and
- Remembering your preferences and application progress.

11.1 Necessary Cookies

In accordance with UK data protection law, we may use certain cookies without explicit consent where they are necessary for:

- Website functionality and user experience.
- Security and fraud prevention.

11.2 Your Choices

You can manage your cookie preferences through your browser settings or our cookie preference centre. However, disabling certain cookies may affect the functionality of our recruitment platform.

12. CHILDREN'S DATA PROTECTION

12.1 Special Protections:

Where our recruitment process may involve candidates aged under 18 years of age (such as graduate or apprentice programmes), we implement additional safeguards including:

- Age-appropriate language and processes.
- Enhanced privacy protections.
- Parental consent where required by law and
- Additional consent requirements where applicable.

We design our recruitment processes to consider the protection and welfare of young candidates throughout the application process.

13. DATA SECURITY

We implement appropriate technical and organisational measures to protect your personal data against unauthorised access, alteration, disclosure, or destruction.

13.1 Security Measures

These include encryption, access controls, staff training, secure data transmission, and regular security assessments.

13.2 Data Breach Notification

In the event of a personal data breach that poses a risk to your rights and freedoms, we will notify you and relevant authorities as required by applicable law, including the Information Commissioner's Office (ICO) within 72 hours where feasible.

14. COMPLAINTS AND CONTACT INFORMATION

14.1 Data Protection Team

For any data protection queries, concerns or complaints, as requested by the Information Commissioner's Office (ICO), please contact us in the first instance. Here's how:

Contact Details:

- **Email:** dataprotection@oneadvanced.com
- **Post:** Data Protection Team, OneAdvanced Limited, The Mailbox Level 3, 101 Wharfside Street, Birmingham. B1 1RF (United Kingdom).

14.2 Complaint Handling

If a complaint arises, speak to the talent acquisition partner handling your recruitment in the first instance or email talentacquisition@oneadvanced.com.

We are committed to resolving data protection complaints promptly. We will:

- Acknowledge your complaint within thirty (30) days of receipt.
- Investigate your complaint thoroughly and impartially.
- Respond without undue delay with our findings and any remedial action taken.
- Provide regular updates on complaint progress where investigations are complex. and
- Ensure complaints are handled by appropriately trained personnel with data protection expertise.

14.3 Regulatory Complaints

You have the right to lodge a complaint with the ICO in the UK or your local data protection authority if you are not satisfied with our response. The easiest way to contact the ICO is via their website - [Contact us - public | ICO](#). However, please permit us the chance to respond to your complaint in the first instance, as directed by the ICO.

15. APPROPRIATE POLICY DOCUMENT

15.1 Schedule 1 Conditions

Where we process special category data under Schedule 1 conditions of the DPA 2018, we maintain an appropriate policy document that includes:

- Which Schedule 1 conditions we are relying upon.
- What procedures we have in place to ensure compliance with the data protection principles.
- How we will treat special category data for retention and erasure purposes.
- A review date and
- Details of an individual assigned responsibility for the processing.

16. ADDITIONAL JURISDICTION-SPECIFIC PROVISIONS

Additional rights and provisions may apply based on your location. Please contact our Data Protection Team for information about rights specific to your jurisdiction.

17. CHANGES TO THIS NOTICE

We may update this privacy notice from time to time to reflect changes in our practices, technology, legal requirements, or other factors.

18.1 Notification of Changes

We will notify you of material changes by posting the updated notice on our website and, where appropriate and possible to do so, during your next interaction with our recruitment systems.

18.2 Effective Date

This privacy notice was last updated 27th January 2026 with immediate effect
