

NEWDAY CANDIDATE PRIVACY NOTICE

NewDay is committed to protecting the privacy and security of your personal information. This privacy notice describes how we collect and use personal information about you in accordance with the General Data Protection Regulation (GDPR).

What is the purpose of this document?

NewDay is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. As someone who is applying for work with us (whether as an employee, worker or contractor) this Privacy 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 the General Data Protection Regulation ((EU) 2016/679) (GDPR).

Data protection principles

We will comply with data protection law and principles, which means that your 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.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept securely.

The kind of information we hold about you

In connection with your application for work with us, we will collect, store, and use the following categories of personal information about you:

- The information you have provided to us in your curriculum vitae and covering letter.
- The information you have provided on our application form, including name, title, address, telephone number, personal email address, gender, marital status, employment history, salary and benefits, right to work details, details of any disability and any reasonable adjustments requested.
- Details of your qualifications, skills, experience and employment history.
- Information about your current level of remuneration, including benefit entitlements.
- Information about your entitlement to work in the UK.
- Any information you provide to us during an interview.
- Any psychometric test results and associated reports.
- Any results from technical assessments.

- Any results from behavioural assessments (e.g. assessment centres).
- Any information provided to support your screening process, including first name, middle name, surname and name history, gender, contact number, email address, date of birth, address history, NI number, mother's maiden name, country of birth, town of birth.
- Any information about Company Directorships.
- Information from our screening process as set out below.
- Details of nationality, and

We may also collect, store and use the following "special categories" of more sensitive personal information:

- Information about your health, including any medical condition or disability.

How is your personal information collected?

We collect personal information about candidates from the following sources:

- You, the candidate.
- Recruitment agencies, from which we collect the following categories of data: name, title, address, eligibility to work in the UK, current/most recent employer, current salary & compensation details, desired salary, gender, marital status, any disability and details of any adjustments required.
- UK and Overseas credit reference agencies, from which we collect the following categories of data: name and aliases, 5 years address history declared and undeclared, active CCJs, satisfied CCJ, and insolvency data, including discharged insolvencies.
- DBS/Disclosure Scotland and relevant overseas bodies in respect of criminal convictions.
- Your named referees, from whom we collect the following categories of data: employment dates, position held, basic salary on leaving, reason for leaving, competence, sickness records, disciplinary records and general information on your performance including attitude and quality of work.
- The information from former employers for Regulatory References
- Fraud prevention agencies such as CIFAS for details of any previous fraud committed against an organisation.
- Academic institutions to validate information you have provided.
- Information from publicly accessible sources.

How we will use information about you

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

- Assess your skills, qualifications, and suitability for the role.
- Carry out background and reference checks once a job offer has been made.
- Communicate with you about the recruitment process.
- Keep records related to our hiring processes.

- Comply with legal or regulatory requirements.

NewDay will process personal data during the recruitment process to assess and confirm your suitability for employment and decide whether to enter into a contract with you.

We also need to process your personal information to decide whether to enter into a contract of employment with you or as required by law or regulatory requirements and in some instances to respond to and defend against legal claims.

Having received your CV, covering letter and our application form, and the results from any test taken we will then process that information to decide whether you meet the basic requirements to be shortlisted for the role. If you do, we will decide whether to invite you for an interview. If we decide to invite you to an interview, we will use the information you provide to us at the interview to decide whether to offer you the role. If we decide to offer you the role, we will then take up references and carry out a criminal record, credit referencing, employment or personal referencing, fraud checks, proof of right to work, any additional regulatory checks required and any overseas checks before confirming your appointment.

If you fail to provide personal information

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, where we require a credit check or references for the role and you fail to provide us with relevant details, we will not be able to take your application further.

How we use particularly sensitive personal information

We will use your particularly sensitive personal information in the following ways:

- We will use information 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.

Information about criminal convictions

We will collect information about your criminal convictions history if we would like to offer you a role (conditional on checks and any other conditions, such as references, being satisfactory). We will use information relating to criminal convictions as permitted by applicable law and in line with our Vetting Policy.

Automated decision-making

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making.

Data sharing

Why might you share my personal information with third parties?

We will only share your personal information with the following third parties for the purposes of processing your application: recruitment or search consultancies, assessment providers, credit/criminal/referencing agencies, academic institutions, suppliers who undertake background screening on our behalf. All our third-party service providers and other entities in the group 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.

Data security

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need-to-know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected data security breach, and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

Transferring Data Outside the EEA

We may transfer your personal information to countries outside the EEA where we need to carry out overseas background checking as part of the recruitment process. We process personal information outside the EEA where such country has an adequacy finding from the EC, we have put Model Clauses in place or the company processing the personal information has signed up to the EU-US Privacy Shield.

Data retention

How long will you use my information for?

We will retain your personal information for a period of 7 months after we have communicated to you our decision about whether to appoint you to the role. We retain your personal information 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. After this period, we will handle your personal information in accordance with our data retention policy

If we wish to retain your personal information on file, on the basis that a further opportunity may arise in future and we may wish to consider you for that, we will write to you separately, seeking your explicit consent to retain your personal information for a fixed period on that basis.

Rights of access, correction, erasure, and restriction

Your rights in connection with personal information

Under certain circumstances, by law you have the right to:

- **Request access** to your personal information (commonly known as a "data subject access request" or "DSAR"). This enables you to receive a copy of the personal information we hold about you
- **Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure** of your personal information. This enables you to ask us to delete or remove personal information we hold about you in specific circumstances.
- **Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation that makes you want to object to processing on this ground.
- **Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy.

- **Request to port some of the personal information we hold about you**

If you want to make a DSAR, review, correct or request erasure of your personal information, object to the processing of your personal data, or request that we provide you with a copy of your personal information in machine readable format so you can port it easily, please contact people@newday.co.uk in writing.

Right to withdraw consent

If you have provided consent to us processing your personal information at any point during the recruitment process you have the right to withdraw your consent for processing for that purpose at any time. To withdraw your consent, please contact people@newday.co.uk. Once we have received notification that you have withdrawn your consent, we will no longer process your application and we will handle your data in line with our retention policy.

Data protection officer

We have appointed a Data Protection Officer (DPO) to oversee compliance with this privacy notice. If you have any questions about this privacy notice, or how we handle your personal information, please contact the DPO at dpofficer@newday.co.uk.

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.