Applicant Privacy Notice

Scope

This policy applies to all candidates wishing to apply to positions within Neos Networks. However, the information we will process about you will vary depending on your specific role and personal circumstances.

Purpose

As an employer we must meet contractual, statutory and administrative obligations. We are committed to ensuring that the personal data collected from individuals is handled in accordance with the principles of privacy legislation.

This privacy policy tells you what to expect when we collect personal information about you.

Neos Networks is the controller for this information unless this notice specifically states otherwise.

Objectives

The objective of Neos Networks is to maintain and continually improve data protection processes to ensure compliance is achieved with all appropriate privacy legislation.

Values

Ambition Simplicity Service Expertise Teamwork Safety

Colin Sempill

CEO

Vicky Bori

Human Resources Director

The Details

In this policy we will tell you:

- How do we obtain your information?
- What personal data we process and why
- Lawful basis for processing your personal data
- How long we keep your personal data
- Data sharing
- Do we use any data processors?
- Transfers of personal data
- Your rights in relation to this processing

How do we get your personal data

We get information about you from the following sources:

- Directly from you
- From an employment agency
- From external job sites
- From an existing employee

What personal data we process and why

We collect and use the following information during our recruitment process.

- Personal contact details such as your name, address, contact telephone numbers (landline and mobile) and personal email addresses
- Information about your current level of remuneration, including benefit entitlements
- Whether you have a disability for which we may need to make reasonable adjustments during the recruitment process
- Information about your entitlement to work in the UK
- Special categories of data such as gender, ethnicity, religion and sexual orientation that is collated into a report to ensure that we are recruiting in a diversified way
- Additional information such as national insurance number and bank details, but only if you successfully secure and accept an offer of employment (the national insurance number will also be inputted to commence a higher security clearance check if relevant to your role)
- We will hold all interview notes and documentation that we collate from you during the recruitment interview and/or assessment stages for 6 months.
- Your date of birth
- A copy of your passport or similar photographic identification and/or proof of address documents to confirm right to work
- Current driving licence
- Marital status for reporting purposes
- Employment and education history including your qualifications, job application, employment references,
- Security clearance details including basic checks and higher security clearance details according to your role

Lawful basis for processing your personal data

Depending on the processing activity, we rely on the following lawful basis for processing your personal data

- Processing necessary for the performance of a contract.
- Processing so we can comply with our legal obligations as your employer.
- Processing in order to protect your vital interests or those of another person.
- Processing for the performance of our public task.

- Processing for the purposes of our legitimate interest.

How long we keep your personal data

Unsuccessful candidate data is held for 6 months and successful candidate information for the retention periods within the Company Retention Policy

Data Sharing

In some circumstances, such as under a court order, we are legally obliged to share information. We may also share information about you with third parties including government agencies and external auditors.

If your application is successful, we may contact past employers to obtain references for you and other third parties as part of the pre-employment screening process. This may include academic institutions, credit reference agencies, occupational health service providers, criminal records bureaus and the DVLA. We may also share your information with third party suppliers who carry out pre-employment screening on our behalf. We will always ask for your consent before processing this type of data.

Do we use any data processors?

Yes - a list of our current data processors is available by contacting dataprotection@neosnetworks.com

Transfers of personal data

We don't routinely transfer employee personal data overseas but when this is necessary, we ensure that we always have appropriate safeguards in place.

This means that we will:
(a) ensure that the country in which your personal information will be handled has been deemed "adequate" by the European Commission under Article 45 of the General Data Protection Regulation (GDPR).
(b) include standard data protection clauses approved by the European Commission for transferring personal information outside the EEA into our contracts with those third parties (these are the clauses approved under Article 46.2 of the GDPR); or

Your rights in relation to processing

As an individual you have certain rights regarding our processing of your personal data, including a right to lodge a complaint with the Information Commissioner as the relevant supervisory authority. The ICO contact details are:
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Helpline number: 0303 123 1113
ICO website: https://www.ico.org.uk

There are also other rights that you may exercise:

1. The right to be informed - Individuals have the right to be informed about the collection and use of their personal data, one of the ways we do this is by having this policy.
2. The right of access - Individuals have the right to access and receive a copy of their personal data, and other supplementary information.
3. The right to rectification – individuals have the right to have inaccurate personal data rectified or completed if it is incomplete.
4. The right to erasure – Individuals have the right to have personal data erased. This is also known as 'the right to be forgotten'. This right isn't absolute, and Data Controllers can still keep personal data, for instance, if they have a legal right.

5. The right to restrict processing - Individuals have the right to request the restriction or suppression of their personal data. This is not an absolute right and while processing is restricted personal data can be stored but not used. This is generally used, for instance, when the right to erasure or object is being investigated.
6. The right to data portability – Individuals have the right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.
7. The right to object – Individuals have the right to object to the processing of their personal data in certain circumstances.
8. Rights in relation to automated decision making and profiling – An individual has the right to request a human being to intervene when a decision has been made by an automated decision-maker.

To exercise any of your rights please contact dataprotection@neosnetworks.com