Group Recruitment Privacy Notice DPN003 V1.1 April 2019

This Countrywide privacy notice provides information on how Countrywide processes the personal data of applicants and potential employees in accordance with Data Protection legislation and regulations (including the General Data Protection Regulation and Data Protection Act 2018).

Countrywide is the "controller" for the purposes of data protection law. That means that we are responsible for deciding how we hold and use personal data about you.

Countrywide Group and its affiliates (Countrywide), is a leading provider of property management and financial products and services, operating in over 1,200 locations across more than 50 brands, with over 11,000 employees within the UK and Ireland.

The Countrywide head office can be located at:

Countrywide House
6 Caldecotte Lake Business Park
Caldecotte Lake Drive
Caldecotte
Milton Keynes
MK7 8JT

Contact number: 01908 465250

1 Types of information collected.

Personal data means any information relating to a living individual who can be identified (directly or indirectly) in particular by reference to an identifier (e.g. name, NI number, employee number, email address, physical features). It can be factual (e.g. contact details or date of birth), an opinion about an individual's actions or behaviour, or information that may otherwise impact that individual in a personal, or business capacity.

Data protection law divides personal data into two categories: ordinary personal data and special category data. Any personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health conditions, sexual life or sexual orientation, or biometric or genetic data that is used to identify an individual is known as special category data (the rest is ordinary personal data).

Categories of personal information collected and processed by Countrywide may include, but are not limited, to:

- Name
- Gender
- Residential status – including present and past addresses
- Date of Birth
- Marital status
- National Insurance number
- Entitlement to work in the UK

- Employment history – including former employer information
- Copies of identification
- Contact information
- Bank account details
- Interview notes

Countrywide may also collect and process special category and criminal offence data, including, but not limited to:

- Health and medical history
- Ethnicity and race
- Criminal offences / convictions

1.1 Methods of collection

Countrywide may obtain information directly from you or from third parties such as, recruitment agencies, job boards, occupational health professionals, previous employers and employee vetting providers.

Such information will generally be collected directly via:

- Your CV
- Application forms
- During correspondence via email, mail or telephone conversations
- During an interview
- From identification documents, such as passport or driving license

We may also obtain information about you from publicly available sources such as your LinkedIn profile or any other social media sources.

You may also agree to third parties disclosing information about you to us, such as references supplied by former employees, however, this would only be requested following an offer for employment to yourself.

1.2 Purposes and lawful basis of processing

We process your personal information for various recruitment reasons as outlined below;

- Article 6, 1 (c) GDPR - Compliance with a legal obligation. This may include:
    - Compliance with employment laws
    - Confirming eligibility to work in the UK, in line with immigration laws
    - Identity verification
    - Disclosure and Barring Service (DBS) checks
    - Credit and sanctions checks

- Article 6, 1, (f) GDPR - Pursuant to our, or a third parties, legitimate interests. This may include:
    - Communication and engagement
    - Recruitment and role suitability
    - Conduct and capability checks
    - Network and information security
    - Data analytic studies (recruitment trends)

We also process special category data, reliant upon the following lawful basis of processing as outlined below;

- Article 9, 2, (f) GDPR - Establishing, exercising or defending a legal claim. This may include:
    - Litigation against the business
    - Fraud prevention and investigation

- Schedule 1, Part 1, (1) DPA 2018 - Performing or exercising obligations in connection with employment. This may include:
    - Health assessments to comply with the Equality Act 2010

- Schedule 1, Part 2, (8) DPA 2018 - Equality of opportunity. This may include:
    - Equal opportunities and diversity monitoring and reporting

We may also process Criminal conviction data reliant upon:

- Schedule 1, Part 3, (33) DPA 2018 - Legal Claims. This may include:
    - Legal or potential legal proceedings, obtaining legal advice or establishing, defending and / or exercising legal rights

2 Information we share

We will only share your personal data with third parties where we have an appropriate legal ground under data protection law which permits us to do so. We do not sell or otherwise disclose personal information we collect about you, except as described in this Privacy Notice. We may share the information we collect with:

- Internal employees for the purpose of the recruitment process

- Formally contracted service providers to support, maintain and host information systems
- Recruitment agencies for recruiting assistance
- Legal and professional advisors relating to legal and financial obligations as an advisor or in the course of a disciplinary or court orders
- Occupational health providers for the capacity of working to be assessed
- Her Majesty's Revenue and Customs for tax purposes
- Home Office for immigration purposes

We may also share information about you, if required legally, to prevent harm or financial / reputation loss, for investigation of suspected or actual fraudulent or illegal activities.

Only information necessary for the provision of a service is provided to third parties and this often occurs following the offer of employment. We contractually require service providers and processors to safeguard the privacy and security of personal information they process on our behalf in line with Data Protection obligations, and authorise them to use or disclose the information only as necessary to perform services on our behalf and under our instruction or to comply with legal obligations and requirements.

2.1 International Transfers

Some of our external third parties are based outside the EEA so their processing of your personal data will involve a transfer of data outside the EEA.

Sometimes, Countrywide will have to transfer your personal data to third party suppliers fulfilling or providing administrative, technical or operational services outside the EEA as it is the case when we transfer data to WNS Global Services Private Limited in India, to process your application. We do this specific transfer under a specific contract approved by the European Commission, which give personal data the same level of protection it has in Europe (Standard Data Protection Clauses for the transfer of personal data to third countries).

Where we are unable to rely on one of the safeguards outlined below, we will rely on the derogation under Article 49 of the GDPR (when the transfer relates to the performance of a contract and for your benefit), and you hereby allow us to do so. Where your personal data is transferred outside the EEA, controls on data protection may not be as wide as the legal requirements within the EEA.
For any other transfer of personal data outside the EEA, we ensure a similar degree of protection is applied by ensuring at least one of the following safeguards is implemented:

(a) We will only transfer personal data to countries that have been deemed to provide an adequate level of protection for personal data by the European Commission (Adequacy Decision).

(b) Where we use certain service providers, we may use specific contracts approved by the European Commission or by the Supervisory Authority, which give personal data the same level of protection it has in Europe (Standard Data Protection Clauses for the transfer of personal data to third countries).

(c) Where we use providers based in the USA, we may transfer data to them if they are part of the Privacy Shield which requires them to provide similar protection to personal data shared between the Europe and the USA (Privacy Shield).

(d) Where we use providers within Countrywide Group, we may transfer data to them under the mechanism of binding corporate rules approved by the Supervisory Authority (BCRs).

2.2 How long do we keep information for?

Information is retained in line with its purpose of processing and only for as long as necessary. Most information is kept for no longer than 1 year following your application; however, this may be extended dependent upon any legal obligations or legitimate interests Countrywide may be required to comply with.

If your application for employment is successful, personal data gathered during the recruitment process will be transferred to your personnel file and retained during your employment in line with our Group Data Retention & Destruction Policy.

Details regarding how your information is processed in relation to employment purposes are provided in a separate notice following acceptance of a job offer.

2.3 Your Rights and Choices

Under Data Protection law you have a number of rights. The applicability of these rights are dependent upon our purpose and lawful basis of processing, therefore not all of these rights may be available to you.

You can exercise your rights either verbally or in writing. However, should you make a request verbally we recommend that you follow this up in writing to provide a clear correspondence trail.

We have an obligation to respond within one month of receiving your request. Should we deem the request to be complex the response time can be extended by up to two months. Should this be required, you will be informed of the extended response date, alongside an explanation, within the original one month time frame.

Should we feel the need to verify your identity, identification will be requested within the one month time frame and only limited to what is necessary for confirmation. Once we are satisfied we will then process your request.

Should we refuse to comply with a request we will inform you of this within the one month time frame and provide an explanation outlining our justification, our internal complaints procedure and your right to complain to a supervisory authority and to enforce your rights through a judicial remedy.

2.5 Your right of Access

You have the right to request and receive copies of the personal information we hold that directly relates to you. This right is applicable at all times; however, due to exemptions within the legislation you may not always receive all the information we process. If this is applicable an explanation will be provided to you within our response.

If you are requesting information on behalf of someone else we require you to provide proof that you are entitled to act on behalf of the data subject and will require written confirmation of this authority. If we are not satisfied you have the right to act as a delegated authority we reserve the right to refuse the request.

2.6 Your right to Rectification

You have the right to request that inaccurate information is rectified and incomplete information completed. Please provide an overview of the information you wish to be rectified / completed. Upon receipt of your request an investigation will be undertaken and a response determining our decision will be provided to you. Please be aware that we may need to take certain steps to verify the accuracy of the new information before the change can be applied.

2.7 Your right to Erasure

You have the right to request your personal information is deleted by us; however, this only applies in certain circumstances. To exercise this right, please provide us with an overview of the information you would like deleted and your reasoning. Upon receipt this matter will be investigated and a response determining our decision provided to you.

In certain circumstances we may be unable to physically delete your data, however, we may put in place steps to ensure the data is 'put beyond use', anonymised or pseudonymised and you will be notified of this.

2.8 Your right to Restrict Processing

You have the right to request we restrict the processing of your personal information; however, this only applies in certain circumstances. To exercise this right please provide us with an overview of the information you would like restricted and your reasoning for this request. Upon receipt this matter will be investigated and our decision provided to you.

2.9 Your right to Object

You have the right to object to us processing your data whereby we are processing your information for our legitimate interests. To exercise this right, please provide us with an overview of the information you are objecting to and your reasoning for this. Upon receipt, this matter will be investigated and our decision provided to you.

Note that these rights are not absolute and in some circumstances we may be entitled to refuse some or all of your request.

3 How to contact us / Complaints and Feedback

You can exercise your rights, raise a query or concern, report a breach or make a complaint by:

Emailing:
Privacy@Countrywide.co.uk

Writing to:
Group Data Protection Officer
Countrywide House
88-103 Caldecotte Lake Drive
Caldecotte Lake Business Park
Caldecotte
Milton Keynes
MK7 8JT

To assist us in responding to your request in a timely and satisfactory manner please provide as much detail as possible during your contact with us.

3.1 How we protect personal information

The security of your personal information is of the utmost importance and Countrywide is committed to protecting the personal data we process. We maintain administrative, technical and physical safeguards designed to protect against accidental, unlawful or unauthorised destruction, loss, alteration, access, disclosure or use. We use SSL encryption on a number of our websites from which we transfer certain personal information.

We take measures to destroy or permanently de-identify personal information if required by law or the personal information is no longer required for the purpose for which we collected it.

In addition, information regarding application and recruitment is maintained on a central system in which access is restricted only to those who have a legitimate business need, and data processed by third parties is only done so under strict instruction from Countrywide, as per the terms of their contract.

Procedures are in place to ensure breaches, or suspected breaches, are dealt with in a timely and secure manner and applicable notification applied within the required timeframes.

4 How to lodge a complaint

If you remain unsatisfied with the way in which Countrywide have handled your data or dealt with your request / complaint you have a right to raise this with the relevant Supervisory Authority and to enforce your rights through a judicial remedy.

UK

Information Commissioners Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel: 0303 123 1113

Website: https://ico.org.uk/concerns/

The ICO currently recommends you contact them within 3 months of your last contact with us.

Ireland

Data Protection Commission
21 Fitzwilliam Square South

Dublin 2
D02 RD28
Ireland

Tel: +353 (0)761 104 800

Website: www.dataprotection.ie

5 Updating this privacy statement

This notice does not form part of any offer of employment and we may amend it at any time to reflect any changes in the way in which we process your personal data.

September 2019