HR Privacy Notice

Introduction

This privacy notice is designed to provide information about our practices concerning the collection, use and disclosure of personal information in the course of our employment practices. During the course of our employment practices we collect, store and process personal information about prospective, current and former employees, partners and workers. Personal information is any data from which an individual can be identified.

Who are we?

Browne Jacobson is made up of Browne Jacobson LLP and Browne Jacobson Ireland LLP. When we mention 'Browne Jacobson', 'we', 'us' or 'our' in this privacy notice, we are referring to the relevant business responsible for processing your data. You will be informed which entity is processing your personal data as your employer, however your personal data may be processed by the other business from time to time.

Please read this notice carefully and contact us if you have any queries by emailing us at: humanresources@brownejacobson.com or by writing to:

The People Director
Browne Jacobson LLP
Castle Meadow Road
Nottingham
NG2 1BJ
+44 (0)115 976 6000
+44 (0)115 947 5246

This privacy notice may change from time to time so we recommend that you review it periodically. This version of the privacy notice was last updated in February 2023.

Who this privacy notice applies to

This privacy notice applies to all persons whose personal information we collect and process in connection with our employment practices. This includes applicants, employees (and former employees), workers (including agency and casual workers and contractors), partners (and former partners), and those carrying out placements and work experience.

Information we may collect and process

In order to carry out our employment practices we process data in relation to:

- Contact details (including names, addresses, telephone numbers, email addresses, national insurance number and emergency contacts)
- Employment records (including professional membership/registration, SRA checks, references, proof of eligibility to work, security checks, photos and exit interview data)
- Recruitment information (such as CVs, interview notes and assessment material)
- Information about performance (such as the ongoing review cycle, performance measures including performance management/improvement plans, learning and development records, continuous professional development records)
- Disciplinary or grievance records
- Contract/Deed information (such as start dates, hours worked, location, current post, previous roles and remuneration information, bank/building society details)
- Work absence information (such as the type of absence (e.g. maternity, sickness) number of absences and reasons (including information regarding physical and/or mental health), holiday records)
- Information about pension arrangements (and all information included in these necessary to administer them) and other benefits we provide as an employer (such as income protection and private health insurance)
- Medical information (including information of any physical or mental conditions and any occupational health information)
- Personal demographics (including: images, age, gender, gender reassignment, racial or ethnic origin, religious or philosophical beliefs, and data concerning sexual orientation and identity.
- Offences (including alleged offences), criminal proceedings, outcomes and sentences and the results of DBS checks
- Employment Tribunal proceedings
- Any accidents, incidents or complaints

We use different methods to collect personal information from and about you, including:

Direct interactions

You may voluntarily provide us with your personal information, for instance when you:

- fill out an application form as part of our recruitment process
- fill out new starter forms as part of our onboarding process
- provide documentation to support our pre-employment checks, for example evidence of your right to work

- correspond with us by email or post
- speak to us in person or on the phone
- give us feedback (for example, by completing a survey);
- register for one of our online learning tools webinars or other events

Information may also be provided by your manager or peers.

Third party sources

We may collect personal information from the following third-party sources:

- as part of the recruitment process – for example from a recruitment agency or assessment provider
- when a pre-employment check is required - for example, this might be from a previous employer or educational institution for the purpose of gathering a reference, from a regulatory body, background check provider, or from government departments such as UK Visas and Immigration (UKVI) or the Disclosure & Barring Service (DBS)

Automated technologies or interactions

As you interact with our website, we will automatically collect information about your browsing activities and your equipment. We collect this information by using cookies. For full details about our use of cookies, please see our Cookie Notice.

We are trained to handle your information correctly and protect your confidentiality and privacy. Your personal information may be stored in different places, including in your electronic personnel file, our HRIS (PeopleXD), Objective Manager and in other IT systems including our email system. These systems are secure and only those who require access to carry out their job role are authorised to access this information. Your information is never sold for commercial purposes and only processed for marketing purposes where we have your consent to do so.

Your information is never sold for commercial purposes and only processed for marketing purposes where we have your consent to do so.

How we use and disclose personal information

We process personal information in connection with our employment practices for the following purposes:

- Recruitment (including in relation to verifying immigration status and/or eligibility to work in the UK, undertaking pre-employment checks and obtaining references)
- Administration and management (including for payroll and performance purposes and for the provision of benefits)
- Performance management
- Pensions administration

- Business management and planning
- Accounting and auditing
- Complying with our legal obligations, such as in relation to safe working practices and compliance with equalities legislation
- Crime prevention and prosecution of offenders
- Learning and development, including continuous professional development records
- Fraud prevention
- Where required in connection with any actual or proposed reorganisation, merger, sale, joint venture, assignment, transfer or other transaction relating to all or any portion of our business or assets
- Research

When processing personal data we comply with the data protection principles and our own data protection policy. We will only disclose the personal data we receive in connection with our employment practices where necessary and where we are satisfied that the data will be adequately protected. Third parties we disclose such data to include:

- Government, statutory, regulatory or other similar bodies or authorities when required or instructed to do so (including in relation to immigration control);
- Other companies within the business;
- Approved third party service or product providers acting on our behalf, for example in relation to payroll or occupational health;
- Our professional advisers;
- Universities and other research partners;
- Potential buyers of the business or merger partners (although where possible that information will be anonymised and the recipient will be bound by confidentiality obligations).

Where we engage third parties to process personal data on our behalf, we do so on the basis of a contract that is compliant with data protection legislation and requires that those third parties will only process your personal data on our written instructions, are under a duty of confidentiality, and are obliged to implement appropriate technical and organisational measures to ensure the security of your personal data.

- We may transfer personal data outside the UK or the EEA where adequate protection measures are in place in compliance with data protection laws.
- We share your personal data within the business. This will involve transferring your data outside the UK or the EEA, as applicable.
- Whenever we transfer your personal data outside the UK or EEA, as applicable, we ensure that at least one of the following safeguards is in place, as applicable:

- Adequacy decision, as approved by the European Commission or the UK government, as applicable;
- Permitted derogation for specified circumstances;
- Processor binding corporate rules;
- Standard contractual clauses, as approved by the European Commission or the UK government, as applicable.

How long we keep personal information

We retain personal data in accordance with our retention and destruction schedule, a copy of which can be found here.

How we protect personal information

We are strongly committed to data security and take appropriate steps to protect the personal information we hold from unauthorised access, loss, misuse, alteration or corruption. We have put in place physical, electronic and managerial procedures to safeguard and secure that information. Further details can be found in our data protection policy.

The legal basis on which we process personal information

Data protection law requires us to have a legal basis for processing your information. In most cases we will only process your personal information:

- So we can carry out our contract with you, or take any steps you ask us to before entering into a contract with you;
- As necessary to perform or exercise any legal rights or obligations we have under the law relating to employment, social security or equalities;
- Where necessary for our legitimate purposes in undertaking our employment practices;
- Where we have your consent.

When processing personal data we comply with the data protection principles and our own data protection policy. By doing so, we consider that the interests and fundamental freedoms of people whose personal data we process do not override the pursuit of our legitimate interests in relation to our employment practices.

Whilst the majority of processing of personal data in relation to our employment practices will not require consent, we will inform you if your consent is required and seek that consent before any processing takes place. In the limited circumstances where you have provided your consent to the

collection, processing and transfer of personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time.

In most cases we process personal data that falls into one of the special categories specified by the General Data Protection Regulation where necessary to perform or exercise our legal rights and obligations under the law relating to employment, social security or equalities, for the purposes of occupational medicine or for the establishment, exercise or defence of legal claims. We may also process special category data where necessary in your vital interests and where you are unable to give consent.

Where we process special category data for the purposes of monitoring or business analysis we will do so on an anonymised basis.

Rights of data subjects

If we process your personal data, you have a number of rights. You may request a copy of the personal data we hold about you (and request that that data be provided in a portable format) and you may object to our processing of it or ask us to rectify it, restrict the way in which we process it or erase it from our records. For further information about your rights, or how to exercise them, please contact us using details above.

Should you have any issues, concerns or problems in relation to your data, or wish to notify us of data which is inaccurate, please let us know by contacting the Legal Director - Risk & Compliance in the first instance by using the contact details below. If we are unable to resolve your concerns and you remain dissatisfied, you have the right to complain to the relevant supervisory authority.

In the UK the relevant supervisory authority is the Information Commissioner's Office (ICO). The ICO's contact details are available here: https://ico.org.uk/concerns.

In Ireland the relevant supervisory authority is the Data Protection Commission (DPC). The DPC's contact details are available here: www.dataprotection.ie.

Representatives

Our UK representative is Browne Jacobson LLP. You may contact our representative at:
Mandy Cooling, Risk & Compliance Director
Browne Jacobson LLP
Castle Meadow Road
Nottingham
NG2 1BJ
or by emailing compliance@brownejacobson.com
or by calling us on +44 (0)115 976 6000 or +44 (0)115 947 5246.

Our EU representative is Browne Jacobson Ireland LLP. You may contact our representative at:
Jeanne Kelly, Partner
Browne Jacobson Ireland LLP
2 Hume Street
Dublin 2
D02 FT82
or by emailing jeanne.kelly@brownejacobson.com