

A woman with short grey hair and glasses is smiling while looking at her smartphone. She is wearing a light-colored blazer over a white top. The background is a blurred office environment with glass partitions and desks.

Employee Privacy Notice

Notice last updated: November 2023

We are committed to protecting your privacy when dealing with your personal information.

This privacy notice provides details about the information we collect about you, how we use it and how we protect it. It also provides information about **Your rights**.

If you have any questions about how we handle your information, please contact us at dataprotection@bupa.com.



Page Navigation



1. [Information about us](#)



2. [What this privacy notice covers](#)



3. [How we collect personal information](#)



4. [Types of personal information](#)



5. [What we use your personal information for](#)



6. [Legal grounds](#)



7. [Legitimate interest](#)



8. [Sharing your information](#)



9. [Transferring information outside the UK and European Economic Area \(EEA\)](#)



10. [How long we keep your personal information](#)



11. [Your rights](#)



12. [Data protection contacts](#)



1. Information about us

In this privacy notice, 'we', 'us' and 'our' mean The British United Provident Association Limited and its subsidiaries (the 'Bupa Group'). For company contact details, click [here](#).

The Bupa Group company you work for, as shown in your employment contract or terms of engagement, makes decisions about how your information is handled.



2. What this privacy notice covers

This privacy notice applies to current and former employees. If you are applying for a different role with us, you should also read the [Applicant Privacy Notice](#). In this privacy notice, references to 'employees' include our permanent and temporary employees, bank and agency workers, and self-employed contractors but do not include self-employed health professionals such as dental associates. If you are a health professional, please read the [Health Professionals Privacy Notice](#). We may give you further privacy information, if necessary, for specific reasons.



3. How we collect personal information

We collect personal information from you and the people and organisations listed below.

You must provide most of this personal information so that we can meet our obligations, you can enjoy the benefits that we offer, and we can manage our relationship with you properly. If you do not provide this personal information, these outcomes may not be possible.

If you provide us with information about other people (for example, your emergency contacts or beneficiaries), you must make sure that they know you are doing this and do not object to you giving us their information. You should also make them aware of this privacy notice.

We collect personal information from you if you provide this in the course of carrying out your role, taking part in rewards or other benefits programmes or through your interactions with us generally, including by phone, by email, through our websites, on our apps, by post, by taking part in assessments (for example, psychometric assessments such as online personality tests), by filling in application or other forms (for example, an international remote working request), on social media or intranet networks, face-to-face (for example, in interviews, appraisals and so on), in the course of virtual meetings or recordings, or by entering competitions.

We also collect personal information about you by monitoring your access to our premises (such as from CCTV, door entry systems and workplace health screening), your use of our devices and systems, and your use of personal devices (if you use these for work).

Our *Acceptable Use Policy* and *Social Media Policy* (available [here](#) or by [contacting us](#)) provide more information about our monitoring. We only carry out monitoring as permitted or required by law and as necessary and justifiable.

We collect personal information about you from other people and organisations such as:

- Your agents (for example, a recruitment agency, trade union representative or legal representative);
- Your referees (for example, your former employer);
- Any service providers who work with us in relation to your employment (for example, selection companies and providers of online assessments);
- Your parent or guardian, if applicable;
- Doctors, other clinicians and healthcare professionals, hospitals, clinics and other healthcare providers to help with workplace health and safety;
- Your Colleagues (for example your Manager);
- Our agents (for example, our legal representatives if we are involved in legal proceedings against you);
- Government departments (for example, the tax office or social security office);
- Credit reference agencies, fraud detection agencies, criminal history reference agencies, if we need to carry out relevant checks (we will tell you at the time if we collect information from you to carry out these checks, and there is more information in the 'criminal offence information' section below);
- Sources which are available to the public, such as:
 1. During your employment, we may check your activity on publicly available social-media networks, such as Facebook, Twitter and YouTube, if we have reason to suspect that you have broken our Social Media Policy (available [here](#) or by [contacting us](#)); and
 2. After you leave your employment with us, we may look at your LinkedIn page to confirm that you are keeping to any restrictions in your contract.



4. Types of personal Information

We process the following types of personal information about you and (where this applies) your dependants.

- **Standard personal information** (for example, information we use to contact you, identify you or manage our relationship with you).
- **Special categories of information** (for example, health information in connection with medical or carer's leave, health information in connection with workplace health screening, information about race, ethnic origin and religion for diversity and inclusion purposes).
- **Criminal offence information** (for example, information relating to criminal convictions and offences, or related security measures). We collect this in line with our local Employment Screening Policies and Candidate's Guides to Bupa Employment Check Standards (available [here](#) or by [contacting us](#)).

Standard personal information includes:

- Contact information (for example, your name, username, address (including any international remote working address), email address and phone numbers);
- The country you live in, your age, your date of birth, sex or gender, employee ID, and national identifiers (for example, your National Insurance number, passport number or driving licence number), your nationality, your right to work in the UK and any other countries where you may remotely work from and travel information (including time spent in each country and right to travel to/from such locations);
- Information about your employment (for example, interview notes, the date you were hired, the dates of any promotions, the dates and details of your resignation or termination, performance appraisals (if this applies), assessments, absence forms, records of training, investigation and disciplinary matters, conflicts of interest);

- Details of your previous work and your education, professional certificates and registrations, other information from your CV and employment references;
- Financial details (for example, payment details and bank details, present and past salary, rewards, expenses claimed);
- The results of any background checks (not including criminal history checks) we have carried out on you in line with our local *Employment Screening Policies* and *Candidate's Guides to Bupa Employment Check Standards* (available [here](#) or by [contacting us](#));
- Photographs and videos from our CCTV systems; the times when you enter and leave our offices (which we collect from our door entry systems); logs of your use and access to our systems and devices; and image/voice recordings of meetings or events; and
- Complaints, incidents and reports you have submitted or have been involved in.

Special category information includes:

- Information about your physical or mental health (you might provide this information when filling in application forms, it may also come from notes and reports about your health and any treatment and care you have received or need, medical certificates, results of psychometric assessments, or information we collect during workplace health screening (such as using thermal imaging or checking your temperature);
- Information about the physical or mental health of the person you are caring for, if you take or ask to take carer's leave;
- Information about your race, ethnic origin, sexual orientation and religion (this information may be included in application forms or by adding to your profile on Workday - you do not have to provide it but if you do we use it on an aggregated basis to support diversity and inclusion initiatives); and
- Information about your disability or long-term health condition (this information may be included in application forms, or you may choose to reveal it during your employment including by adding it to your profile on Workday, to allow for any required adjustments as well as support diversity and inclusion initiatives and reporting on an aggregated basis).



5. What we use your personal information for

We process your personal information to:

- Manage the recruitment process and our relationship with you, our business and the people and organisations who provide services for us;
- Provide learning, development and training to our People;
- Protect our (or our customers' or other people's) rights, property or safety, including to maintain a safe working environment;
- Exercise our rights, to defend ourselves from claims, to keep to laws and regulations that apply to us and the people and organisations we work with and comply with our obligations arising from the employment contract;
- Take part in, or be the subject of, any sale, merger or takeover of all or parts of the Bupa business; and
- Consider and act upon whistleblowing reports we receive, as set out in our local *Speak Up Policies* (available [here](#) or by [contacting us](#)).





6. Legal Grounds

By law, we must have a lawful reason for processing your standard and special category personal information for the purposes listed in section 5. These are set out below.

Standard personal information:

- It is necessary to meet the obligations set out in a contract or to take steps before entering into a contract – if we have a contract with you, we will process your personal information to fulfil that contract (for example, to pay you for your service or services);
- It is in our own or a third party's legitimate interests (see section 7 for more details); or
- We have to or are allowed to do so by law (for example, in line with employment and social security laws and to meet requirements from our regulators).

Special category information:

- It is necessary for carrying out our obligations and exercising specific rights under employment, social security or social protection law or to meet our regulatory requirements (for example, we process health and disability information in connection with managing ill health or disability benefit schemes and assessing whether you are fit for work, for insurance purposes and to manage sickness and absence, and we process information about your race, ethnic origin, sexual orientation, religion or philosophical beliefs to help us monitor equal opportunities and comply with regulatory requirements);
- It is necessary in the vital interests of you or another person (for example, if you need medical attention at work and are unable to communicate or give your consent);
- You have obviously made that personal information public (for example, you publicly share sensitive personal information on social media);
- It is in the public interest, in line with local laws;
- It is necessary to establish, make or defend legal claims;
- It is necessary for the purposes of occupational medicine, including to assess whether you are able to work; and
- You provide clear and specific consent to take in certain psychometric assessments, such as online personality tests (please note, we don't need specific consent for all psychometric assessments).

Criminal offence information

For some roles we need to carry out criminal history checks, so we may process criminal offence information. Our legal ground for carrying out these checks depends on which part of the business you work in, but typically it is because it is necessary to keep to employment law or other legal requirements such as those under financial services legislation and legislation relating to protecting vulnerable groups.



7. Legitimate Interest

Legitimate interest is one of the legal reasons why we may process your personal information. Taking into account your interests, rights and freedoms, the types of legitimate interest which allow us to process your personal information include:

- To find the best talent and make sure new employees are ready to do their jobs;
- To build the capability of our employees to help our organisation grow, now and in the future;
- To reward our employees in a way that attracts and helps us keep the best in the market;
- To provide our employees with support on a full range of day-to-day employment matters, and to otherwise manage our relationship with you, our business and people and organisations who provide services on our behalf;
- To make sure we are set up for success and to deliver our strategic vision through strategic resource planning, including planning for restructures and earmarking people for certain roles ready for when other employees leave the organisation;
- To protect our (or our customers' or other people's) rights, property or safety, including to protect the health, safety and welfare of workers, and to maintain a safe working environment;
- To exercise our rights, to defend ourselves from claims and to keep to laws and regulations that apply to us and the people and organisations we work with; and
- To take part in, or be the subject of, any sale, merger or takeover of all or parts of the Bupa business.



8. Sharing your information

We share your information, for the purposes set out in this privacy notice, with:

- Other members of the Bupa Group;
- Doctors, clinicians and other healthcare professionals, hospitals, clinics and other healthcare providers to help with workplace health and safety;
- Your pension scheme;
- Debt collection agencies (UK wide);
- Our insurers;
- Our agents (for example, our legal representatives, translators, interpreters and tax advisers in line with the law);
- Suppliers who help deliver products or services on our behalf or who give us advice;
- Any corporate clients you provide services to onsite, if your role involves this;
- People or organisations we have to or are allowed to share your personal information with by law (for example, for fraud prevention or safeguarding purposes, including with the Care Quality Commission, and social security and tax offices);
- Other individuals where required when responding to their right of access requests;
- Our regulators, including the Care Quality Commission, who may access care records and other personal information as part of their work (their privacy notice is available at www.cqc.org.uk/about-us/our-policies/privacy-statement), the Financial Conduct Authority and the Prudential Regulation Authority, as well as bodies and associations our people belong to;
- the NHS Wales Shared Services Partnership if you work for a Welsh Bupa Dental Care practice as we share workforce data via the Wales National Workforce and Reporting System (WNWRS);
- The police and other law enforcement agencies to help them perform their duties, or with others if we have to do this by law or under a court order; and
- If this applies, potential buyers of all or part of our business.

If we share your personal information, we will make sure appropriate protection is in place in line with data protection laws.



9. Transferring information outside the UK and the European Economic Area (EEA)

We deal with many international organisations and use global information systems. As a result, we transfer your personal information to countries outside the UK and the EEA (the EU member states plus Norway, Liechtenstein and Iceland), for the purposes set out in this privacy notice.

We take steps to make sure that, when we transfer your personal information to another country, appropriate protection is in place in line with data protection laws. Often, this protection is set out under a contract with the organisation who receives that information. For more information about this protection, please contact us at

dataprotection@bupa.com.



10. How long we keep your personal information

In general, we will keep your information for seven years after the date you leave your employment. However, there may be circumstances that mean we must keep your personal information for longer. For example, if there was an ongoing tribunal, court or another type of proceeding, we would keep your information until the end of those proceedings and any possible appeals, and the end of any relevant claims periods. We will keep your information for the period needed to meet our legal responsibilities. We use the following criteria to help us decide how long we need to keep your personal information for.

- Whether you are currently employed by us.
- How long it is reasonable to keep records to show we have met the obligations we have to you and by law.
- Any periods for keeping information which are set by law or recommended by regulators, professional bodies or associations.
- Any time limits for making a claim.
- Any tribunal, court or other relevant proceedings that apply.
- How long it would be reasonable to expect you to reapply for a job or, if you are employed by us, to ask for a reference.

At the end of the period worked out using the above criteria, we will securely and permanently delete the personal information in your file. If you would like more information about how long we will keep your information for, please contact us at dataprotection@bupa.com.

We are committed to keeping your information secure and will store it in line with our *Enterprise Security Policy* (available [here](#) or by [contacting us](#)).



11. Your rights

Under European and UK data protection laws, you have the following rights relating to the information we hold about you in some computer and paper records.

- **Right of access:** You have the right to make a written request for details of the personal information we hold about you and a copy of that personal information.
- **Right to rectification:** You have the right to have inaccurate information about you corrected.
- **Right to erasure ('right to be forgotten'):** You have the right to have certain personal information about you deleted from our records.
- **Right to restriction of processing:** You have the right to ask us to use your personal information for restricted purposes only.
- **Right to object:** You have the right to object to us using personal information.
- **Right to data portability:** You have the right to ask us to transfer personal information you have given us to you or someone else in a format that can be read by computer.
- **Right to withdraw consent:** We do not normally rely on permission to allow us to process your personal information. We will only ask for your permission in very limited circumstances and, if we do so, we will make it obvious to you when we are asking for permission and what it is for. You have the right to withdraw any permission you have given us to handle your personal information. If you withdraw your permission, this will not affect the lawfulness of how we used your personal information before you withdrew your permission.

These rights may not apply in all cases. If we are not able to meet your request, we will explain why. If you make a request, we will ask you to confirm your identity if we need to, and to provide information that helps us to understand your request better. If you would like more information about your rights, or to exercise any of your rights, please contact us at dataprotection@bupa.com.



12. Data protection contacts

If you have any questions, comments, complaints or suggestions relating to this notice, or any other concerns about the way in which we process information about you, please contact our Data Protection Officer and Privacy Team at dataprotection@bupa.com.

You also have a right to make a complaint to your local privacy supervisory authority. Our main office is in the UK, where the local supervisory authority is the Information Commissioner.

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
United Kingdom
SK9 5AF

Website: www.ico.org.uk Phone: 0303 123 1113 (local rate) or 01625 545 745 (national rate)

In Ireland, the local supervisory authority is the Data Protection Commission.

Data Protection Commission

Fitzwilliam Square South

Dublin 2

D02 RD28

Ireland Website: <https://www.dataprotection.ie/>

Email: info@dataprotection.ie

You can also make a complaint with another supervisory authority which is based in the country or territory where:

- You live;
- You work; or
- The matter you are complaining about took place

