# Employee Privacy Notice

Last updated: December 2025

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

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 (available here in Workvivo under Privacy). We may give you further privacy information, if necessary, for specific reasons.

## 3. How we collect your personal information

We collect personal information from you and the people and organisations listed on the following page.

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 effectively manage our relationship with you. 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 Standard and Social Media Policy 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);
- 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, for example:

- 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.
- 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. What personal information we collect

| | |
|---|---|
| Basic personal details | Name, employee ID, age, date and place of birth, gender, marital status |
| Contact Information | Username, address (including any international remote working address), email address and phone numbers, relationship to your emergency contacts and beneficiaries |
| Residency | The country you live in, national identifiers such as national insurance number, passport number, or driving licence number |
| Nationality | Your nationality, your right to work in the UK and in any other countries from where you remotely work including visa information, the time you have spent in such countries, and your right/permission to travel to/from such locations |
| Employment details | Your current and previous role(s), the Bupa entity you work for, 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 including absence reasons, records of training, investigation and disciplinary matters, information about conflicts of interest (including relationships and any directorships you may hold) |
| Work and education | Details of your previous work and your education, professional certificates and registrations, military service information, other information from your CV and employment references. This also includes details of your learning records during your employment |
| Communications | Details of any contact we've had with you including complaints and incidents |
| Financial details | Your present and past salary, rewards, expenses claimed, payments and bank account details, information about tax and social security payments |
| Background checks | The result of any background checks we have carried out on you |
| Systems logs | Logs of your use and access to our systems / devices as described in the Acceptable Use Standard |
| Images and audio | Photographs and videos from our CCTV systems, or video/audio recordings of meetings or events, images and videos you submit as part of internal competitions, testimonials or engagement initiatives |
| Site access data | Door entry systems records e.g. the time you enter, leave, move around our premises |
| Special category information | Personal Data relating to your physical and mental health, genetic or biometric data, sex life, sexual orientation, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership. Medical Information and Diversity Information form part of Special Categories of Personal Data |
| Criminal offence information | Information about unspent criminal convictions, spent criminal convictions (to the extent permitted by law), and criminal charges pending |
| Diversity Information | Information about religious beliefs, health information (including disability), sexual orientation, race, ethnicity, and socio-economic background. |
| Medical Information | Dates of absence, reason for absence, medical information / reports, fit note information, immunisation records, diagnosis information, prognosis information, pre-employment medical assessment and details of accommodations and adjustments |

## 5. What we use your personal information for

In the table below we have described the various purposes for which we process your personal information and outline the typical types of information we use for these purposes. Under data protection law we also need to tell you what lawful ground we rely on when using your information.

| Purpose | Description | Type of information | Our lawful ground |
|---|---|---|---|
| Manage payments | To pay your salary, bonus, expenses and to deduct tax and social security amounts. | ▪ Basic personal details<br>▪ Contact information<br>▪ Financial details | ▪ Performance of employment contract |
| Employee monitoring | We monitor employee use of Bupa assets to detect unauthorised use. See the Acceptable Use Standard for more information.<br><br>If needed we will also review Site Access Data and CCTV if unauthorised activity is suspected. | ▪ System logs<br>▪ Communications<br>▪ Site access data<br>▪ Images and audio<br>▪ Contact information | ▪ Performance of employment contract<br>▪ It's required or allowed by law<br>▪ We have a legitimate interest to validate and identify you when you access our systems and applications, identify fraud and fraudulent activity, identify individuals accessing our premises |
| Disciplinary matters and investigations | Gathering, handling and assessing evidence relating to possible grievance or disciplinary matters and associated hearings. | ▪ Basic personal details<br>▪ System logs<br>▪ Communications<br>▪ Site access data<br>▪ Images and audio<br>▪ Employment details | ▪ It's required or allowed by law, including but not limited to: anti bribery and corruption laws and regulations, anti-money laundering laws and regulations, facilitation of tax evasion laws and regulations; whistleblowing laws and regulations<br>▪ Performance of employment contract<br>▪ We have a legitimate interest to manage our employment relationship with you |
| Exercising our rights, to defend ourselves from claims | Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work. | ▪ Basic personal details<br>▪ Contact information<br>▪ Employment details<br>▪ Any other type of personal information outlined above as relevant | We have a legitimate interest to exercise our rights and defend ourselves from legal claims. |
| Equal opportunities monitoring | We monitor the diversity of our applicants, successful candidates, existing workforce including senior manager positions, for the purpose of promoting the diversity of individuals holding these positions. | ▪ Special category data | It's required or allowed by law |

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

| Purpose | Description | Type of information | Our lawful ground |
|---|---|---|---|
| Engagement and wellbeing- | To manage feedback you share with us for instance, via the Employees as Customers platform and People Pulse.<br><br>To promote or ensure employee engagement and wellbeing, including through campaigns, competitions and events. | ▪ Basic personal details<br>▪ Contact information<br>▪ Special category information | ▪ We have a legitimate interest in promoting and ensuring employee engagement and wellbeing. |
| Criminal record checks | For some roles we need to carry out criminal history checks. We will tell you when these checks are performed. It is usually at the start of employment and as required to meet regulatory requirements such as the Fitness and Probity regime in Ireland and the Senior Management Conduct Regime in the UK. | ▪ Basic personal details<br>▪ Criminal offence information | ▪ This depends on which part of the business you work in, but typically it's because it's necessary to adhere to employment law or other legal requirements such as those under financial services legislation and legislation relating to protecting vulnerable groups. |
| Health and safety | To protect 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 (including to allow for any required adjustments). | ▪ Basic personal details<br>▪ Contact information<br>▪ Employment details<br>▪ Special category data | ▪ It's required or allowed by law |
| Data analytics | To conduct data analytics studies to review and better understand employee retention and attrition rates | ▪ Employment details | ▪ We have a legitimate interest to optimise our employee engagement and manage our business |
| Performance management | To ensure we manage employee productivity and performance within our business. This may include monitoring both the behaviour and activity of our employees and the use of our systems. | ▪ Employment details | ▪ We have a legitimate interest to manage our employment relationship with you |

## 6. Sharing your personal information

We've set out the groups of Bupa teams and external parties with which we collect and share information and our reasons for doing so. Please note that we may also disclose your personal information to third parties other than those listed where we are required or permitted to do so by law.

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

| Bupa team / external party | Our reasons |
|---|---|
| Within Bupa:<br>▪ People Function departments, including leaders and team members;<br>▪ local, and executive management, or other Bupa employees on their behalf, responsible for managing or making decisions in connection with your relationship with Bupa or when involved in a People Function process concerning your relationship with Bupa (including, without limitation, colleagues from Company Secretarial, Compliance, Legal and so on);<br>▪ colleagues in the Pension function and other areas relating to the provision of colleague benefits;<br>▪ system administrators;<br>▪ Group Tax, Treasury, Finance, Internal Audit and IT departments, and the Global People Function information systems support team where necessary for the performance of specific tasks or system maintenance<br>▪ Personal information may also be shared with certain interconnecting systems such as recruitment, local payroll, benefits and IT systems.<br>▪ Certain basic Personal Data, such as your name, location, job title, contact information and any published skills and experience profile may also be accessible to other employees for the purposes set out in the Privacy Notice. This includes your profile on our HR System such as Workday for example. | ▪ Governance and reporting<br>▪ Exercising our rights and defend ourselves from claims<br>▪ Enabling our employees' access to global Bupa systems<br>▪ Complying with applicable laws and regulations<br>▪ Incident management |
| Doctors, clinicians and other healthcare (HC) professionals, hospitals, clinics and other HC providers | ▪ Provision and receipt of services<br>▪ Management of relationships<br>▪ Complying with applicable laws and regulations<br>▪ Incident management |
| Debt collection agencies (UK wide) | ▪ To recover monies owed to us |
| Third party that buys or takes over any of our businesses, i.e.:<br>▪ Potential buyers or sellers of businesses and assets we are buying or selling<br>▪ Third parties that assume responsibility for Bupa | ▪ Potential buyers or sellers of businesses and assets we are buying or selling<br>▪ Third parties that assume responsibility for Bupa |
| Any corporate clients you provide services to on site, if your role involves this | ▪ Client relationship management |
| Suppliers: We use many suppliers to provide our services. We put measures in place to ensure that our suppliers process your personal information fairly and in line with our expectations. Examples of suppliers are: providers of people management platforms or whistleblowing services; travel management providers; benefit providers; IT software providers; professional consultants such as solicitors, auditors, tax advisors | ▪ Help us run our business<br>▪ Support us to manage our business and meet our regulatory obligations<br>▪ Gain advice on business decisions and strategy |

## 6. Sharing your personal information (continued)

| Bupa team / external party | Our reasons |
|---|---|
| Public sector bodies, government and regulatory organisations: people or organisations we have to, or are allowed to, share your personal information with by law such as:<br>▪ Government and their agencies<br>▪ Law enforcement agencies like the Police<br>▪ Authorities and regulatory bodies such as the Financial Conduct Authority (FCA) or Prudential Regulation Authority (PRA)<br>▪ Data protection supervisory authorities<br>▪ HM Courts and Tribunals Service<br>▪ HMRC<br>▪ Care Quality Commission<br>▪ General Medical Council<br>▪ General Dental Council<br>▪ The Health & Care Professions Council<br>▪ Disclosure & Barring Service<br>▪ The Nursing and Midwifery Council<br>▪ The United Kingdom Council for Psychotherapy<br>▪ The British Association for Counselling and Psychotherapy<br>▪ Responsible Officer<br>▪ NHS Wales Shared Services Partnership if you work for a Welsh dental practice as we are required to share workforce data via the Primary Care Workforce Intelligence System;<br>▪ And any others that are relevant to you | ▪ Comply with our legal and regulatory obligations<br>▪ Protect our rights |
| Public data sources<br>▪ During your recruitment, we may look at your LinkedIn page to get an overview of your professional history and qualifications, and we may also read any work you have had published that is relevant to the role we are considering you for, such as research or academic articles;<br>▪ 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.<br>▪ 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.<br><br>Note: In this case we only collect information about you. | ▪ Validate our records<br>▪ Check our employees are of good standing and quality, and investigate possible fraudulent activity or complaints |

## 7. 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 that receives that information. For more information about this protection, please contact us at dataprotection@bupa.com.

## 8. 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 is 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 information retention period, 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.

## 9. Your rights

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

- **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. For example, we may not be able to share all the information we hold about you in response to a right of access request since confidential references are exempt from disclosure.

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 ukpeopleoperations@bupa.com.

## 10. 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 Digital and Data Protection 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. Their details are available here.

In Ireland, the local supervisory authority is the Data Protection Commission. Their contact details are available here.

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