

**GDPR TEMPLATE:**

**EMPLOYEE PRIVACY NOTICE**

**Points to note**

* Before using this template Employee Privacy Notice, it is essential that you read these ‘Points to note’, together with the separate document, ‘Make UK Essential GDPR Templates for HR – Points to note’, which provides important information applicable to all of the template documents, including the Privacy Notice.
* This template Privacy Notice is designed to comply with the GDPR requirement for you to be transparent with your Employees (as defined in the body of the document) and to provide them with required information about your processing activities, i.e. to explain to them what you do with their personal data. There is a detailed list of information that must be included in the Privacy Notice, all of which is covered in this template.
* This template is for the main Employee Privacy Notice, which you should provide to your current Employees and to your new Employees when they commence employment. It assumes that you have a separate Privacy Notice for job applicants (see Make UK’s GDPR Template: Job Applicant Privacy Notice). Strictly, where an individual provides you with personal data, you should provide them with the required information about your processing activities at that time (i.e. ‘just in time’). However, the nature of the employment relationship means that you will be receiving and processing new personal data from your Employees on a regular basis and therefore if you issue an Employee Privacy Notice that includes the required information about a particular type of data, then we do not think you need to reissue the document every time Employees provide you with new data of that type.
* That said, in the interest of ensuring fair and transparent processing, you may also wish to repeat or cross-refer to the information that is in the template at the time you collect new data in certain situations, e.g. on a form that collects new data or in a policy that is handed out to an Employee at the time that the application of that policy is triggered. In addition, you may need to provide more specific privacy notice information at the time you collect new data, where particular elements of the data processing are not covered by the main Employee Privacy Notice. (Again, this information could be included on a form that collects new data or in a policy that is handed out to an Employee.) Both of these practices are also a way of ensuring that the required information is provided ‘just in time’.
* There is no ‘one size fits all’ when it comes to producing an Employee Privacy Notice. Each employer must consider what is to be included in the context of its own business requirements/operations. It is therefore essential that you customise the template Employee Privacy Notice to reflect the types of personal data that you hold and how you process them.
* Note that the Tables in the Appendix to the template document will require particularly careful tailoring. The categories of personal data set out in the Tables mirror those in the Employee sections of the Record of Processing, since that document is a record of what an employer does with personal data. They include the types of personal data that we think most employers will hold and process in relation to their Employees, and the Tables describe the purposes for which we think most employers will process the data, the third parties with whom we think most employers will share data, etc. However, you will need to adapt the text to ensure that all the information matches what actually happens in your own organisation. (The results of any audit you have conducted will help you to do this.)
* This template Employee Privacy Notice avoids, wherever possible, referring to consent as a legal ground for processing personal data. This is because, as highlighted in the UK GDPR and the Information Commissioner’s Office (ICO) guidance, it generally won’t be appropriate to rely on consent in the employment context, given the power imbalance in the employment relationship. (Consent should only be used in the employment context if it is genuinely voluntary – i.e. Employees who refuse or withdraw their consent will not suffer in any way or be subject to any detriment, however minor. If an employer doesprocess any Employee data on the basis of genuinely voluntary consent, it could provide the required information about consent as a legal ground for processing, and the right to withdraw consent, in a ‘just in time’ privacy notice at the time it seeks the consent.)
* The template takes into account the (somewhat conflicting) GDPR requirements for a privacy notice to give detailed, specific information to individuals, and to provide it in a concise, intelligible, accessible form. We have taken a ‘middle ground’ approach to the level of detail we have included in the document, and we have sought to aid Employees’ understanding by providing more generic summary information in the body of the document and then including more specific and detailed information in the Appendix, using tables to link certain of the information where it is sensible to do so (e.g. the type of data, what it is used for and the legal grounds for use).
* A privacy notice must include information on how long you are going to retain personal data or, where you cannot specify the retention period, details of the criteria you take into account when deciding how long to retain personal data. In the template Employee Privacy Notice (in the Appendix to the document), we suggest certain retention periods for various categories of personal data (referred to as ‘Guideline Retention Periods’). Where we anticipate that you would want to avoid giving a particular time period, we state that the retention period will be ‘decided on a case by case basis in accordance with the criteria set out in this Privacy Notice’. The body of the document (see ‘How long will we keep your personal data?’) lists our suggested criteria for setting retention periods, which include the limitation periods for common Employee claims and certain key statutory retention requirements. Not only do the criteria apply where there is no specific retention period but also they are key when deciding on the Guideline Retention Periods.
* Since this template Privacy Notice is an employee-facing document, we aim to ease the administrative burden on you as an employer in this regard and keep this document as user-friendly as possible for all Employees by suggesting that you provide for various, relatively broad, categories of Employee personal data and adopt longstop guideline retention periods for them. The template explains to Employees that the Guideline Retention Periods set out in the Appendix are the *longest* period for which you will *ordinarily* keep Employees’ personal data and that particular items of personal data will, where possible, be kept for shorter periods. In any event, in order to help you comply with the GDPR obligation not to keep personal data for longer than necessary for the purposes for which it was processed, we suggest underpinning the retention information given in this document by more detailed internal processes/guidance for HR which break down some categories of data further and suggest retention periods on a more granular/stricter basis – we have produced the template Employee Data Retention Process for this purpose. Further information about the application of retention periods, and the differences between those provided in an Employee Privacy Notice and those in an internal process, is set out in the Employee Data Retention Process.
* Even though the suggested Guideline Retention Periods in the Appendix to this Privacy Notice are longstop dates, you do still need to consider whether the periods are suitable for your company and to tailor them where you need to, taking into account the criteria set out in the document (and/or any other criteria you come up with) in the context of your particular organisation. (For example, if your organisation works with particular regulated substances, then your statutory retention obligations may mean you have to provide for longer retention periods for some records). In addition, you must ensure that the Privacy Notice is an accurate reflection of what you do in practice. If your processes and systems currently don’t enable you to delete data as quickly as we have suggested, you may need to set out even longer longstop Guideline Retention Periods to reflect your current practice. However, if you are aiming for stricter compliance, you may wish to work on reducing them going forwards by establishing or improving processes/systems to ensure more efficient data minimisation and update the Privacy Notice once you have done so.
* We have for now presented the Employee Privacy Notice in a text/print-out format. However, depending on the organisation’s technological capabilities, it could be presented in a more user friendly form. In addition, the guidance to the GDPR requires you to consider the most appropriate medium (hard copy, online on your company intranet, etc.) for privacy notices, based on what the individual will most easily be able to access in the circumstances.
* Whether you are introducing a GDPR-compliant Employee Privacy Notice for the first time, or updating your existing one, when presenting this document to Employees and implementing it in your organisation, you must make clear in your communications that this Employee Privacy Notice replaces any previous privacy notice that they may have been given in the past. This could be done, e.g. in cover emails sending Employees links to the Privacy Notice on the intranet, and/or as cover sheets to hard copy Privacy Notices that you distribute to all Employees.
* In order to demonstrate your compliance with the GDPR, you will need to keep a record showing that you have distributed the Employee Privacy Notice to all Employees. If you send out a communication by email, the sent emails could serve as your record. If you provide Employees with hard copies, you will need to create a record – this could be as simple as keeping a list of Employee names together with a note of the date on which they were given / sent each of the documents.
* Finally, note that this template Employee Privacy Notice is intended to comply with the requirements of the UK GDPR and DPA 2018. It is suitable for UK-based employers to issue to Employees in the UK. If you are a UK-based employer that has Employees in the EEA, you are likely to remain subject to the EU GDPR and will need to provide an EU GDPR compliant privacy notice to your Employees in the EEA. A privacy notice that complies with the EU GDPR would need to include the details of your EEA representative if you do not have an office or establishment in the EEA. (See the ICO’s guidance for details of the requirement to appoint an EEA representative: <https://ico.org.uk/for-organisations/data-protection-and-the-eu/data-protection-and-the-eu-in-detail/the-uk-gdpr/european-representatives/>.) There may also be other requirements for the content of a privacy notice under local law in the EEA country where your Employees are located, so we recommend that you take advice on your particular circumstances.

**Customisation**

The following table sets out information to explain the various sections of this template Employee Privacy Notice and assist employers in tailoring particular parts of it for their organisation.

|  |  |
| --- | --- |
| **Section of document** | **Points to note** |
| Who is the controller? | We have included language in square brackets that you can use if you share personal data with your parent/other group companies. This should avoid those companies having to provide your Employees with their own privacy notice. This approach works because there is an exemption from the requirement to provide fair processing information where a controller obtains personal data from someone other than the data subject and the data subject already has the relevant information – i.e. where group company A shares its Employees’ personal data with group company B, group company B does not have to provide a privacy notice to those Employees if the Employee Privacy Notice they have received from their employer (group company A) already informs them about how group company B uses their personal data.  If your parent/other group companies actually collect personal data themselves directly from your Employees and personal data is regularly processed at a group level, you may wish to provide a group notice to cover all such collection and processing, but this would require quite extensive tailoring of this template.  Note that we have assumed that a parent/other group company with whom you share Employees’ personal data will be a controller of that data in their own right, as opposed to a “joint controller” with you. Under the GDPR, controllers are “joint controllers” where they “jointly determine the purposes and means of processing”. There is very limited guidance on precisely what this means. However, unless and until official guidance to the contrary is published, we recommend taking the view that it will apply only very rarely in the employment context. We would say, for example, that where a subsidiary company shares its Employees’ performance appraisal data with its parent company because the parent company runs a group bonus scheme and determines eligibility for performance-related bonus payments, the parent company decides for itself how it processes that data – the subsidiary is not jointly involved in determining the purposes and means of processing. We take this approach because being “joint controllers” introduces an additional administrative burden, as the controllers must determine their respective rights and responsibilities in relation to the personal data they jointly control and must inform data subjects of the “essence” of the arrangement between them.  Note also that you need to include details for a point of contact for Employees if they have questions/concerns. If you have appointed a Data Protection Officer (DPO), their details will be included in this section of the Privacy Notice. If you do not have a DPO, details of another suitable contact person are included in the ‘Your rights’ section of the document (the template lists example positions). |
| What type of personal data do we hold about you? | This section lists types of personal data that you hold about your Employees. The lists of ordinary and special category data include types of personal data that we think most employers will process. It is fine for the lists to be expressed as general categories of personal data. However, you should tailor them to remove reference to any types of personal data you don’t process (and add further types of personal data that you do process, if applicable).  Note that we have for ease of reference included criminal convictions/offences data within the list of special category data; even though this is not technically special category data under the UK GDPR, similar restrictions apply under the DPA 2018. |
| Why do we hold your personal data and on what legal grounds? | Here, we list some common purposes for which employers process Employees’ ordinary and special category personal data. You should ensure that these lists are accurate and complete (i.e. they include all purposes for which you envisage processing Employees’ personal data and they don’t include purposes that don’t apply in your organisation).  We also explain the common legal grounds for processing Employees’ personal data. It’s likely that you will rely on each of these different legal grounds in respect of some of the processing that you do so this list is unlikely to need customising. |
| How do we collect your personal data? | In this section, we explain that most Employee personal data is collected from the Employee directly, or from colleagues/other internal sources in the ordinary course of business.  Where you collect personal data from a source other than the data subject, the GDPR requires the sources of data to be identified. Accordingly, the part of this section that you should pay most attention to when customising is the paragraph detailing external sources of personal data. |
| If you give us someone else’s personal data | Note that, strictly speaking, full compliance with the GDPR would require the employer to give a privacy notice to the individual whose personal data they have received from an Employee. Some employers may prefer not to do this as they perceive the administrative burden of doing so to be disproportionate given the limited use that they will make of such data and – accordingly – the relatively low risk of such use to the individual concerned. This template recognises that this may be employers’ preferred approach and therefore requires Employees to pass on certain minimum information to the individual whose personal data they provide to the employer. However, in some cases, the drafting of an appropriate privacy notice will be fairly simple and employers wishing to get closer to full GDPR compliance may therefore choose to provide one, either directly to the individual or by asking Employees to pass on a copy. This template also includes optional language providing for this. |
| Who do we share your personal data with? | This section simply provides a short summary of common situations in which you might share Employees’ personal data with third parties. Further details about data sharing are contained in the Appendix. |
| Consequences of not providing personal data | The GDPR requires you to specify whether the provision of personal data by the Employee is part of a statutory or contractual requirement or obligation and the possible consequences of failing to provide the personal data. We have set out some examples in square brackets, which should be tailored to ensure they are accurate for your organisation.  You will probably not be able to cover here *all* possible consequences of refusal/failure to provide *every type* of personal data you ask for. The template therefore notes that you will inform Employees about the *particular* consequences of them choosing not to provide requested personal data at the relevant time. (This could be done on a data collection form, or via a ‘just in time’ privacy notice). |
| How long will we keep your personal data? | A privacy notice must include information on how long you are going to retain personal data or, where you cannot specify the retention period, details of the criteria you take into account when deciding how long to retain personal data. Since this template Privacy Notice is an employee-facing document, we aim to ease the administrative burden on you as an employer by adopting generous longstop retention periods and caveats permitting individual decisions on retention where appropriate. See further below for information on the Guideline Retention Periods identified in the Appendix. |
| Profiling/solely automated decision-making | Profiling, or solely automated decision-making, takes place when an electronic system uses personal information to make a decision without human intervention. Under the GDPR, it is only permitted in very limited circumstances.  We do not think very many employers will use profiling to process their Employees’ personal data. However, if you do, you must include information in the Privacy Notice which provides meaningful details about the logic, significance and consequences of doing so. There is an example included in square brackets in the template Privacy Notice to give you an idea of the sort of information that would be required.  You only need to include reference to profiling/solely automated decision-making in the Privacy Notice if you do actually do it in respect of Employee personal data. If you don’t, then you can remove this section – but you must take care to update the Privacy Notice if you introduce profiling/solely automated decision-making in the future. |
| Transferring personal data outside the UK | The obligation to inform Employees about transfers of their personal data outside the UK only applies where such transfers do actually take place. This section of the template Privacy Notice is therefore in square brackets as, if you do not transfer any Employee personal data outside the UK, you will not need to include it. However, you will need to take care that you update the Privacy Notice if you introduce such transfers in the future.  The UK GDPR restricts the transfer of personal data to countries outside the UK unless the country is recognised as providing an adequate level of data protection, appropriate safeguards are in place, or an exception applies.  If you currently transfer Employee personal data to any countries outside the UK, you must identify those countries and provide details of the relevant arrangements:   * With regard to transfers of personal data from the UK to the EEA, the UK Government has recognised the adequacy of data protection provisions in EEA countries. Accordingly, this template Privacy Notice assumes that personal data can flow freely from the UK to the EEA without additional safeguards. * For transfers of personal data from the UK to other countries, the UK Government has recognised the effectiveness of existing European Commission adequacy decisions, so transfers to those countries can continue. (Going forwards, the UK can make its own adequacy decisions. So far, an adequacy decision has been issued in respect of the Republic of Korea (South Korea). In addition, adequacy has been confirmed in respect of organisations in the USA that have signed up to the UK Extension to the EU-US Data Privacy Framework – a binding set of commitments that are enforced in the USA by the Federal Trade Commission.) Transfers to other countries that do not have an adequacy decision (or to organisations in the USA that have not signed up to the UK Extension to the EU-US Data Privacy Framework) require you to conduct a transfer risk assessment and put appropriate safeguards in place, such as the ICO’s International Data Transfer Agreement (IDTA) or its UK Addendum to the EU standard contractual clauses, or binding corporate rules if the transfer is between group companies. Please refer to the ‘Make UK Essential GDPR Templates for HR – Points to note’ for further information about transfer risk assessments and appropriate safeguards.   There are a number of derogations under the UK GDPR that allow transfers of personal data outside the UK in the absence of adequacy decisions or appropriate safeguards. Most of these will not be relevant for Employee personal data. However, there may very occasionally be situations in which an employer would be able to rely on the derogations permitting transfer where it is necessary for the performance of a contract with the data subject, or for the conclusion or performance of a contract made in the interest of the data subject between the controller and another person. For example, if Employees were to go on a one-off business trip to a country which is not recognised by the UK as providing adequate protection for personal data as part of the performance of their duties, the employer may book flights and accommodation on their behalf. Since the employer is essentially a one-off customer of the airline and the hotel, it may not be in a position to suggest that they implement the IDTA as an appropriate safeguard. However, the transfer of the Employees’ personal data to both the airline and the hotel could potentially be viewed as necessary under either of the derogations described above.  We have not included reference to these derogations in this template Employee Privacy Notice, because the ICO guidance states that they should only be relied on exceptionally and not for regular transfers. In addition, it may not be practical to include reference to transfers based on the derogations in your main Employee Privacy Notice – for example, because you cannot identify in advance all of the countries to which Employees’ personal data will be transferred for business travel purposes, and/or because only a small proportion of your Employees will have their personal data transferred in this way. If you find that you need to transfer any Employee personal data internationally on an exceptional basis in reliance on one of these derogations, you could inform Employees about the transfer in a ‘just in time’ privacy notice.  Finally, note that this template Privacy Notice is written from the perspective of a UK-based company, rather than a company based in the EEA or elsewhere, so it provides information about transfers of Employee personal data out of, rather than into, the UK. For further information about transfers of personal data into the UK, please refer to the ‘Make UK Essential GDPR Templates for HR – Points to note’. |
| Your rights | Note that we have not included in the list of Employees’ rights in relation to personal data the right to object to direct marketing, as we assume that most organisations will not be marketing their products directly to their Employees in the workplace/in the context of their work activities. If, however, this is something that you do, you should add reference to this right. |
| Appendix | In the introductory paragraphs to the Appendix, we explain to recipients of the Privacy Notice that not all of the types of personal data listed will necessarily be relevant to them, depending on their role, individual circumstances, etc.  In addition, this template Privacy Notice is drafted to cover all your staff (i.e. not just employees in the narrow sense but also workers, agency workers, self-employed contractors, etc.) and you won’t hold as much personal data for a self-employed contractor as for others, for example.  However, if you regularly engage large numbers of self-employed contractors, or agency workers, for whom many of the categories of personal data listed in this template Privacy Notice would not be relevant, you should consider whether to produce separate privacy notices for them. This would be more in keeping with the GDPR requirement for processing to be fair and transparent, as a privacy notice will be easier for an individual to understand if it only includes information that is relevant for them. |
| Appendix – all Tables | The tables need careful tailoring – ask yourself the following questions:   * Do they include reference to types of personal data that you do not process and should therefore delete, or omit types of personal data that you do process and should therefore add in? * Do the ‘purposes for processing’ match your actual purposes? Do you need to add other purposes (or remove any that don’t apply to you)? * Do they cover all of your legal grounds for processing?   With regard to the Guideline Retention Periods identified in the tables, note the following:   * These Guideline Retention Periods are intended to act as ‘longstop’ dates, i.e. they represent the longest period for which you will typically hold a given type of Employee personal data (although the ‘How long do we keep your personal data?’ section of the body of the Privacy Notice explains that there may be some circumstances in which you need to depart from these periods). * In order to ensure your compliance with the GDPR requirement not to keep personal data for longer than necessary, the longstop retention periods set out here should be underpinned by more detailed internal processes/guidance for HR which break down some categories of data further and suggest guideline retention periods on a more granular/stricter basis – we have produced the template Employee Data Retention Process for this purpose. * Generally, you should not need to extend the Guideline Retention Periods suggested here as we don’t think you would ordinarily need the data for longer than this. But, on the other hand, you must make sure the Privacy Notice is an accurate reflection of what you do. If your processes and systems currently don’t enable you to delete data as quickly, you may need to set out longer periods here to reflect your current practice – but work on reducing them going forwards by establishing or improving processes/systems to ensure more efficient data minimisation, and update the Privacy Notice once you have done so. |
| Appendix – what we use your special category data for | Obvious points to tailor here will include removing reference to trade union membership data and biometric data if you do not actually process these.  Note that with regard to biometric data, none of the special category legal grounds for processing seems to be readily applicable, other than explicit consent. However, in order for consent to be considered truly freely given, you would need to ensure that there is a genuine alternative to the processing of biometric data should an Employee refuse (or subsequently withdraw) their consent. Given that biometric data (e.g. fingerprint or retinal scanning) is most likely to be used by employers to control access to secure equipment or premises, this may not be feasible in practice.  One other legal ground that might be open to you is that the processing is necessary to comply with a legal obligation in relation to employment, though this would very much depend on the circumstances. For example, if biometric data is used to regulate access to dangerous machinery for which operators must be specially trained, you could argue that the use of biometric data to prevent untrained Employees from accessing the machinery is necessary to comply with your legal health and safety obligations.  However, the health and safety argument would not assist if you use biometric data to control access to your administrative offices, for example. In those circumstances, should you nonetheless wish to use biometric data, you would have to:   * take a broader/more bullish view of your legal obligations in relation to employment, e.g. if using biometric data to control access to HR’s office space, reference the duty of trust and confidence and argue that, in order to comply with this, you need to prevent confidentiality breaches/unauthorised access to HR files, although this is somewhat tenuous; or * fall back on (probably invalid) consent – in which case, be aware that this could put you in breach of the GDPR – you would need to assess the risk, e.g. of an Employee complaining to the ICO, and determine whether or not to go ahead.   Note that the information on the processing of criminal offences data in this table assumes that you do not conduct criminal record checks on existing Employees and that your processing of Employees’ criminal offences data is limited to when a criminal conviction comes to light during employment. If you do conduct criminal record checks on existing Employees, you will need to add reference to this here (and you can import appropriate language from the Job Applicant Privacy Notice). However, it is important to be aware that the legal grounds on which employers are able to process Employees’ criminal offences data are very limited and whether or not you are able to do so lawfully under the GDPR may depend on the nature of the Employee’s role – see the ‘Points to note’ on the Job Applicant Privacy Notice for details. |
| Appendix – Who we share your personal data with | The European guidance on transparency (which the ICO recognises remains relevant notwithstanding the UK’s departure from the EU) says that, ideally, any third party providers with whom you share personal data should be named. However, the guidance does allow for a description of categories of provider as an alternative (noting that this should include as much detail as possible). Accordingly, the template allows for either option. Naming your providers would be a higher level of compliance if you feel comfortable and want to do it. However, it does have the disadvantage that you would need to amend the Privacy Notice each time you change provider, so you might prefer to stick to a description of the type of provider instead. You could mix and match, e.g. naming your longstanding providers that are unlikely to change, but describing types of provider where you don’t have such a long-term relationship or where you regularly review service provision and put it out to tender. |

**Employee Privacy Notice**

This Employee Privacy Notice sets out what personal data we, [COMPANY], hold about you and how we collect and use it, both whilst you are working for us and after you have left. It applies to current and former employees, workers, [*contractors, agency workers, consultants, interns, volunteers, partners and directors*] (together referred to as ‘Employees’ or ‘you’).

We are required by data protection law to give you the information in this Privacy Notice. It is important that you read the Privacy Notice carefully, together with any other information that we might give you from time to time about how we collect and use your personal data. You should also read our Data Protection Policy, which explains our obligations in relation to personal data and how we keep it secure, as well as what we expect from you when you are handling personal data in the course of your work.

This Privacy Notice applies from [date], and supersedes any previous versions. It does not form part of any contract of employment, or other contract to provide services that you may have with us and does not give you any contractual rights. We may update this Privacy Notice at any time.

**Who is the controller?**

[*Name of employer*] is the “controller” for the purposes of data protection law (also referred to in this notice as ‘we’ or ‘us’). This means that we are responsible for deciding how we hold and use personal data about you. We can be contacted as follows: [*Contact details*].

[*If you have a Data Protection Officer*: Our Data Protection Officer is [*name and contact details*]. As Data Protection Officer, they are responsible for informing and advising us about our data protection law obligations and monitoring our compliance with these obligations. They also act as your first point of contact if you have any questions or concerns about data protection].

[*If you share any Employee personal data with a group company*: This Privacy Notice also covers how [*name and contact details of any such group company*] uses any personal data about you that we share with them (for more information, see the Table in the Appendix, **Who we share your data with**)]. [*Name of group company*] is the controller of any personal data they hold and use about you. [*If the group company has a Data Protection Officer*: The [*name of group compa*ny’s] Data Protection Officer is [*name and contact details*]. As Data Protection Officer, they are responsible for informing and advising [*name of group compa*ny] about its data protection law obligations and monitoring its compliance with those obligations. They also act as your first point of contact if you have any questions or concerns about data protection in relation to the personal data they hold]. [*Name of group company*] applies the same high standards to data protection compliance as we do.]

**What is personal data?**

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 provides additional protection for personal data about an individual’s racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health, sex life or sexual orientation, criminal convictions or offences, biometrics (if used for identification purposes), or genetics. This is referred to as **special category** **data**. (We refer to personal data that is not special category data as **ordinary personal data**).

**What type of personal data do we hold about you?**

We hold and use various types of ordinary personal data about you, including, for example: biographical details; recruitment information; details of the terms of your employment with us; pay and benefits details; working hours; performance information; details of your holidays and other leave; disciplinary, conduct and grievance matters; employee representation; health and safety; CCTV footage; business equipment, technology and systems usage information, etc.

We hold and use various types of special category data about you, including: sickness absence and medical information; details of family leave which could include information about your health, religious beliefs, sexual life or sexual orientation; equal opportunities monitoring data which could include information about your race or ethnicity, religious beliefs, sexual orientation or health[; trade union membership][; biometric data used to identify you].

**Why do we hold your personal data and on what legal grounds?**

We hold and use your **ordinary personal data** for employment, HR and business administration purposes. This will include, for example: management of our employment relationship with you; administration of pay and benefits; monitoring and assessment of performance; provision and regulation of holidays and other leave; addressing conduct, disciplinary and grievance issues; performance of day-to-day business activities, etc.

Data protection law specifies the legal grounds on which we can hold and use personal data.

Most commonly, we rely on one or more of the following legal grounds when we process your personal data:

* Where we need it to perform the contract we have entered into with you (**performance of the contract**) [whether this is an employment contract, a contract for services or another type of contract]. This may include, for example, ensuring that we pay you correctly and that we provide your contractual holiday entitlement.
* Where we need it to comply with a legal obligation (**legal obligation**). Typically, this may include legal obligations such as the obligation: to provide statutory holidays and statutory family leave and pay (maternity, paternity, adoption, shared parental, etc.); to pay the National Living Wage /National Minimum Wage; to comply with limits on working time; to meet health and safety requirements; not to discriminate or dismiss Employees unfairly.
* Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests (**legitimate interest**). This may include, for example, managing working hours to ensure effective business operations, and monitoring your use of computers or other technology.

We hold and use your **special category data** for purposes including: managing absence and ensuring cover; making adjustments to your job to accommodate health conditions; ensuring your health and safety and that of other Employees; facilitating the taking of family related leave; paying sick pay, maternity, paternity, adoption or shared parental pay as applicable; monitoring equality of opportunity and diversity in our organisation[; paying trade union subscriptions, facilitating meetings with trade union representatives, permitting time off for trade union activities][; ensuring security of laptops/controlling access to our premises].

Since special category data is usually more sensitive than ordinary personal data, we need to have an additional legal ground to use and hold it. Most commonly, as well as one of the legal grounds listed above, we rely on one or more of the following additional legal grounds when we process your special category data:

* Where we need to exercise our legal rights or carry out our legal obligations in relation to employment or social security and the processing is in line with our Data Protection Policy (**legal obligation/right in relation to employment).**
* Where it is needed in the public interest, such as for equal opportunities monitoring [or in relation to our occupational pension scheme], and the processing is in line with our Data Protection Policy (**public interest in monitoring equal opportunities within the workforce**).

Occasionally, we may also hold and use ordinary personal data where needed to protect your vital interests or those of another person. We may also occasionally hold and use certain special category data where, as appropriate: we need it to establish, exercise or defend a legal claim; it is needed in the public interest for the detection or prevention of unlawful acts (or, in respect of data concerning criminal convictions/offences, it is needed for the detection or prevention of unlawful acts); it is needed in the public interest in the area of public health; it is needed to protect your vital interests (or someone else’s) and you are not capable of giving your consent; or you have already made the information public.

Sometimes we may use your personal data for purposes that are different from those for which we collected it. If we do this, we will notify you as required under data protection law.

The Appendix to this Privacy Notice sets out in more detail the types of ordinary and special category personal data we collect and hold about you, what we use it for, who we share it with and the relevant legal grounds under data protection law for doing so in each case.

**How do we collect your personal data?**

You provide us with most of the personal data about you that we hold and use. Other personal data about you we hold and use is generated by you in the course of carrying out your duties. For example, during email correspondence or when producing documents or when you are using certain equipment such as computers, [door entry systems/clocking-in and out systems].

Some of the personal data we hold and use about you is provided by or generated from internal sources during the course of running our business. For example, colleagues may refer to you in emails or documents, your manager will assess you as part of the appraisal process and information about you may be generated as part of our business and operational planning.

Some of the personal data about you that we hold and use may come from external sources. For example: when we offered you a job, we may have collected references from previous employers; we may obtain information about you from publicly available sources such as your LinkedIn profile or other media sources; we may ask for a report from an occupational health professional if you have long-term sickness absence; customers may give feedback about you; we might seek advice from a professional adviser that includes information about you[; or your TU representative might correspond with us in particular situations]. [*Insert any further examples that are particularly pertinent to you.*]

**If you give us someone else’s personal data**

Sometimes, you might provide us with another person’s personal data – e.g. details of your emergency contact or next of kin. In such cases, we require you to inform the individual what personal data of theirs you are giving to us. You must also give them our contact details and let them know that they should contact us if they have any queries about how we will use their personal data[, or, if we ask you to do so, you must pass on to them a separate privacy notice in which we explain what we do with their personal data that we receive from you][, although we may also provide them with a specific privacy notice to give them this information].

**Who do we share your personal data with?**

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. Commonly, this could include situations where we are legally obliged to provide the information (e.g. to HMRC for tax purposes), where it is necessary to comply with our contractual duties (e.g. to providers of your contractual benefits such as [occupational pension, health insurance, etc.]), or where it is necessary in our legitimate interest (e.g. to an IT service provider for maintenance of our IT systems).

Further details of who we share your personal data with, and our purposes and legal grounds for doing so, are set out in the Appendix to this Privacy Notice.

**Consequences of not providing personal data**

We only ask you to provide personal data when we have a good reason and there may therefore be consequences if you do not provide particular information to us.

Some of the personal data you provide to us is required by law. For example, if you do not provide your national insurance number, we will not be able to make correct tax/NI deductions on PAYE, and, if you are pregnant, we require a MATB1 in order to pay statutory maternity pay.

We may require you to provide other personal data, where it is necessary for us [or our pensions/benefits providers] to fulfil our contractual obligations to you, or for you to fulfil your contractual obligations to us, or where our use of the data is necessary in our legitimate interests. For example, [if you do not provide us with a timesheet, we cannot pay you for the [overtime] hours you have worked / if you do not complete the application form for health insurance, we cannot provide you with health insurance / *tailor examples and insert others as appropriate*].

If you choose not to provide us with personal data requested, we will tell you about the particular implications of any such decision at the relevant time.

**How long will we keep your personal data?**

We will not keep your personal data for longer than we need it for our legitimate purposes.

We have put in place internal processes and procedures to assist us in determining the appropriate retention periods for Employees’ personal data and we take into account the following criteria when doing so:

* the amount, nature, and sensitivity of the personal data;
* the risk of harm from unauthorised use or disclosure;
* the purposes for which we process your personal data and how long we need the particular data to achieve these purposes;
* how long the personal data is likely to remain accurate and up-to-date;
* for how long the personal data might be relevant to possible future legal claims; and
* any applicable legal, accounting, reporting or regulatory requirements that specify how long certain records must be kept.

Given the variety of Employees’ personal data that we use and the varying circumstances in which we use it, it is difficult to specify precisely how long we will keep particular items of personal data. Where possible, the Tables in the Appendix to this Privacy Notice identify retention periods (referred to as ‘Guideline Retention Periods’) applicable to various categories of your personal data, which have been determined on the basis of the above criteria and which represent the longest period for which we will ordinarily keep them. There may, however, be circumstances in which it is necessary for us to keep particular items of your personal data for more or less time, taking into account the above criteria.

In addition, for some types of personal data, it is more appropriate to decide retention periods on a case by case basis (also using the criteria described above), and this is indicated in the Tables where applicable.

Please note that personal data that is held on IT back-up data sets for disaster recovery purposes may be retained for a different period. This is because it may not be possible to apply retention periods to individual records without erasing the whole back-up data set. [Back-up data sets are generally retained for up to [3 years] for disaster recovery purposes.]

**[*If you use profiling/solely automated decision-making:* Solely automated decision-making**

Solely automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention. [Provide *meaningful details about the logic, significance and consequences of any automated decision-making processes you operate – for example:* We currently use solely automated decision-making to assess your eligibility for our contractual attendance allowance. We determine your eligibility automatically using our clocking-in and out software based on the times at which you clock in and out of work.]

**[*If you transfer personal data outside the UK:* Transferring personal data outside the UK**

An overseas transfer of personal data takes place when the data is transmitted or sent to, viewed by, accessed by or otherwise used by, a third party in a different country.

Although the UK is no longer a part of the European Economic Area (EEA), the UK Government has recognised the adequacy of data protection provisions in EEA countries. Accordingly, we are able to transfer your personal data to the following EEA [country/countries] without restriction: [*name country/countries*].

[*If you transfer personal data outside the EEA:* Data protection law restricts transfers of personal data to countries outside of the EEA because the law in those countries might not provide the same level of protection to personal data as the law in the EEA. To ensure that the level of protection afforded to personal data is not compromised, therefore, we are only able to transfer your personal data outside the EEA if certain conditions are met, as explained below.

We may transfer [some of] your personal data to the following [country/countries] outside the EEA: [*name country/countries*].

* [*Where there is an adequacy decision in place for the relevant non-EEA country*: There is an adequacy decision [issued by the European Commission and recognised by the UK Government /issued by the UK Government] in respect of [*name country*]. This means that [*name country*] is deemed to provide an adequate level of protection for your personal data.]
* [*Where the transfer is to an organisation in the USA that has signed up to the UK extension to the EU-US Data Privacy Framework:* The organisation(s) in the USA to whom we transfer your personal data have signed up to the UK extension to the EU-US Data Privacy Framework. This is a binding set of commitments that are enforced in the USA by the Federal Trade Commission and which the UK Government has recognised as providing an adequate level of protection for your personal data.]
* [*Where there is no adequacy decision in place for the relevant non EEA country and the UK extension to the EU-US Data Privacy Framework does not apply:* We have conducted a transfer risk assessment and put in place the following appropriate safeguard[s] to ensure that any personal data transferred to [*name country*] is treated in a way that is consistent with and which respects the applicable law on data protection and receives an adequate level of protection: [*specify measure, for example, binding corporate rules, the IDTA, or the UK Addendum to the EU standard contractual clauses*]. If you require further information about [this/these] safeguard[s], [you can request it from [*Name, position, email*]/ it is available [here *LINK*].]]

**Your rights**

You have a number of legal rights relating to your personal data, which are outlined here:

1. **The right to make a subject access request.** This enables you to receive certain information about how we use your personal data, as well as to receive a copy of it.
2. **The right to request that we correct incomplete or inaccurate** personal data that we hold about you.
3. **The right to request that we delete or remove** personal data that we hold about you where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have exercised your right to object to processing (see below).
4. **The right to object to our processing** your personal data where we are relying on our legitimate interest (or those of a third party), where we cannot show a compelling reason to continue the processing
5. **The right to request that we restrict our processing** of your personal data. This enables you to ask us to suspend the processing of personal data about you, for example if you want us to establish its accuracy or the reason for processing it.
6. **The right to request that we transfer** your personal data to you or to another party, in a structured format. This right applies in respect of data that you have provided where our legal ground for using the data is that it is necessary for the performance of a contract or that you have consented to us using it (this is known as the right to “data portability”).
7. **[*Include if you use profiling/solely automated decision-making:* Rights in relation to solely automated decision-making (including profiling),** including the right to voice your opinion, to obtain human intervention in the decision-making, and to contest the decision.**]**.]

If you would like to exercise any of the above rights, please contact [Name/position/email/address]. Note that these rights are not absolute and in some circumstances we may be entitled to refuse some or all of your request.

If you have any questions or concerns about how your personal data is being used by us, you can contact [*if you have a Data Protection Officer*: the Data Protection Officer][*if you don’t have a Data Protection Officer*:the HR Data Protection Lead/ Data Protection Team] [*contact details*].

[*If a group company holds/uses any Employee personal data*:If you have any questions or concerns about how your personal data is being used by [Group company name] you can contact their [*if they have a Data Protection Officer*: Data Protection Officer][*if they don’t have a Data Protection Officer*: HR Data Protection Lead/ Data Protection Team] [*contact details*].

Note too that you have the right to make a complaint at any time to the ICO, the UK supervisory authority for data protection issues. Details of how to contact the ICO can be found on their website: <https://ico.org.uk> **APPENDIX – FURTHER DETAILS**

**This section of the Privacy Notice tells you in more detail about the type of personal data we hold about you, what we use it for, our legal grounds for doing so, who we share it with and how long we keep it.**

Please note that we will not necessarily hold, use or share *all* of the types of personal data as described in this Appendix in relation to you. The specific types of data about you that we will hold, use and share will depend on your role, the terms on which you work for us, your individual circumstances and circumstances affecting the company from time to time. For example, if you do not have a work computer or use any other technical device in your role, we will not hold any computer or device usage records for you; if you work for us as a self-employed contractor, we will not hold records about benefits that you are not entitled to; if you have not yet taken a day off sick, we will not currently hold any sickness absence records for you; and we are only likely to share information about you with professional advisers in particular circumstances.

Note also that the first two Tables below divide items of personal data into relatively broad categories (under the heading “Type of ordinary personal data held by us”, or “Type of special category personal data held by us”). Where multiple purposes and/or legal grounds for our use of a given “type” of personal data are identified, this does not necessarily mean that *all* of the purposes and/or legal grounds are applicable to *all* items of personal data falling within that “type” of personal data.

**More information about your ordinary personal data**

|  |  |  |  |
| --- | --- | --- | --- |
| **Type of ordinary personal data held by us** | **What we use it for** | **Legal ground** | **Guideline Retention Period** |
| Biographical details (including name, title, contact details, DOB, gender, emergency contacts, [photograph]) | Administration of the contract, emergency contact details so we can look after your welfare in an emergency,  gender for [gender pay gap reporting, equal opportunities monitoring],  DOB for [*insert purpose of processing*]  [photograph for ID badges and on intranet/web to help colleagues/customers/ security to identify you] | Legal obligation  Performance of the contract  In our legitimate interest to hold emergency contact details in order to inform a person nominated by you in an emergency situation.  [In our legitimate interest to use photographs to help colleagues/customers/ security to identify you] | During employment and up to 6 years after employment ends  Emergency contacts, [photograph]: during employment and up to 6 months after employment ends |
| Recruitment information (including correspondence/references/ right to work checks and related documents) | Administration of the contract, and to check and demonstrate that you have the legal right to work in the UK | Legal obligation  Performance of the contract  In our legitimate interest to maintain relevant and appropriate records of recruitment for business administration and administration of your employment | During employment and up to 6 months after employment ends  (Right to work checks - two years after employment ends) |
| Employment details (including start date, contractual terms, location, job title, career history with us) | Administration of the contract  Managing our relationship with you on an ongoing basis  Details about role/experience, etc. may be used in communications with customers and potential customers | Legal obligation  Performance of the contract  In our legitimate interest to manage our ongoing relationship and to promote our goods/services to customers and potential customers | During employment and up to 6 years after employment ends |
| Payroll, tax/NI and bank details | Paying you, deducting tax and NI as appropriate, keeping appropriate records | Legal obligation  Performance of the contract | Payroll/tax/NI: Six years from the end of the financial year in which payments are made  Bank details: During employment and up to 6 months after employment ends |
| Working hours and arrangements | Paying you correctly  Complying with legal requirements regarding working time  Managing attendance, day to day operational management and dealing with requests to alter hours | Legal obligation  Performance of the contract  In our legitimate interest to manage working hours/ arrangements to ensure effective business operations | During employment and up to 6 months after employment ends |
| Pay and benefits including pensions [and share incentive schemes] (and information necessary to administer these) and expenses | Providing you with agreed pay, benefits and expenses; making decisions about future compensation; tracking and reviewing pay, benefits, expenses; making strategic decisions about compensation; auditing and reporting on company financial position | Legal obligation  Performance of contract  In our legitimate interest to analyse pay, benefits and expenses and make decisions about appropriate compensation on an individual and company level | During employment and up to 6 years after employment ends *[check with your pension provider what Employee data they need you to retain and for how long]* |
| Performance and career progression (including appraisals, performance management, target/objective setting, consideration of new duties/roles) | Ensuring you perform in accordance with your contract and to the standards we require; considering future duties/roles[; setting performance-related pay increases; determining eligibility for performance bonuses] | Performance of the contract  In our legitimate interest to manage performance and duties/roles to ensure effective business operations [and set appropriate levels of remuneration] | During employment and up to 6 months after employment ends |
| Qualifications (including educational, vocational, driving licences where appropriate) and training | Ensuring you are appropriately qualified and trained for current or potential roles | Legal obligation  Performance of the contract  In our legitimate interest to ensure that you have appropriate qualifications and training for your current or potential future roles | During employment and up to 6 months after employment ends |
| Holidays and other leave, including furlough | Managing statutory and non-statutory holiday and other leave | Legal obligation  Performance of contract  In our legitimate interest to ensure leave taken is compatible with our business requirements and that any consequent operational adjustments are made | During employment and up to 6 years after employment ends |
| Disciplinary, conduct and grievance matters about you or involving you | Investigating and dealing with disciplinary, conduct and grievance matters related to you or otherwise involving you | Legal obligation  Performance of the contract  In our legitimate interest to deal effectively with disciplinary, conduct or grievance matters whether you are the subject of them or are otherwise connected to the issues raised | During employment in accordance with our disciplinary and grievance policies, and up to 6 months after employment ends |
| Employee representation | Establishing and facilitating consultation with [staff forum/works council/ EWC/*insert details of Employee representative body*] on relevant matters | Legal obligation  In our legitimate interest to engage with appropriate Employee representatives on relevant matters | During employment and up to 6 months after employment ends |
| Health and safety | Conducting risk assessments; establishing safety measures to mitigate identified risks; providing a safe working environment; keeping required records;[*add specific requirements – complying with rules about x*]; | Legal obligation  In our legitimate interest to ensure Employees are able to perform their duties in a safe environment for the efficient operation of the business | Decided on a case by case basis in accordance with the criteria set out in this Privacy Notice, in particular any legal requirement to retain particular records |
| Changing terms of employment or termination of employment | Administration of the contract, making changes to the terms of employment to fit business requirements; managing our relationship with you on an ongoing basis including during notice; promotions, role changes and other career progression; termination of the working relationship whether instigated by us or you; managing post–employment issues | Legal obligation  Performance of the contract  In our legitimate interest to manage, alter and, where relevant, to terminate the contractual relationship or respond to resignations and to deal effectively with post-employment issues | During employment and up to 6 years after employment ends |
| CCTV footage | Primarily for security purposes, although we may also use CCTV footage when investigating allegations of misconduct by Employees | Legal obligation  Performance of the contract  In our legitimate interest to deal effectively with allegations of misconduct and to maintain the security of our premises | [*Number*] [days/weeks] after date on which footage was recorded *[complete in accordance with your company policy/practices on CCTV]* |
| Information about your use of business equipment, technology and systems including our computers/ telephones/mobile phones/ software/ applications/ social media/[door entry systems/clocking in and out systems/time recording/performance output monitoring] | Maintaining the operation, security and integrity of our business communications systems (e.g. protection from hackers, malware, etc.); providing IT and communications systems support; preventing excessive personal use; [recording communications with customers for quality control and training purposes; keeping premises secure; managing time; recording rate of work/efficiency of work] | Performance of the contract  In our legitimate interest to maintain operation, security and integrity of communications systems, prevent excessive use of business resources for personal purposes,[and monitor and maintain quality of communications with customers; record time worked and rate/efficiency of work] | [One year] from date information is captured |
| Personal data produced by you and others in the course of carrying out your job (e.g. job-related emails, minutes of meetings, written reports, business social media presence, business cards, etc.) | Performance of job duties by you and your colleagues; carrying on the business of the company; monitoring your business social media presence to ensure you comply with standards expected | Performance of the contract  In our legitimate interest to carry out the company business | Decided on a case by case basis in accordance with the criteria set out in this Privacy Notice |
| Personal data, which may include any of the types of data set out in this Appendix, that is relevant to our strategic decision-making processes, to planning business operations, to any company restructuring or reorganisation, to responding to subject access requests by Employees, customers or others as required by law, actual and potential legal claims, corporate reporting and business risk analysis | To enable us to carry out the company business, analyse current business performance, plan for the future, reorganise or restructure, present information in reports to relevant audiences such as shareholders, respond to subject access requests as required by law, protect the company from legal claims, seek professional advice as and when required in the course of running our business | Legal obligation  Performance of the contract  In our legitimate interest to carry out the company business, including taking strategic decisions in the interest of the business, communicating about the business with relevant audiences and seeking professional advice where appropriate | Decided on a case by case basis in accordance with the criteria set out in this Privacy Notice |

**More information about your special category data**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type of special category data held by us and circumstances in which we use it** | **What we use it for** | **Legal ground** | **Special category legal ground** | **Guideline Retention Period** |
| Sickness absence and medical information (including records relating to absence and its management, information about any medical condition and doctor’s reports and notes [drug and alcohol testing] [records of Covid-19 related self-isolation)] [Covid-19 testing] [Covid-19 vaccination status] | Payment of [company and] statutory sick pay; providing [health insurance and/or *INSERT OTHER BENEFITS*]; managing absence and ensuring appropriate cover;  attendance management;  considering how your health affects your ability to do your job and considering adjustments, which may involve us seeking medical advice on this; compliance with health and safety requirements[; sharing Covid-19 test results with relevant health authorities if required] | Legal obligation  Performance of the contract  In our legitimate interest to manage Employees with health conditions, maintain a safe working environment and to manage sickness absence of our workforce and ensure appropriate cover | Legal obligation/right in relation to employment  In exceptional circumstances, to protect your or someone else’s interests where consent cannot be given  [Processing is necessary in the public interest in the area of public health] | Decided on a case by case basis in accordance with the criteria set out in this Privacy Notice |
| Family leave (including maternity, paternity, adoption and shared parental leave, parental bereavement leave, parental leave and time off for dependents) (which could include information about [your health, religious beliefs, sexual life or sexual orientation]) | Facilitating the taking of family related leave; payment of maternity, paternity, adoption, shared parental, or parental bereavement pay; managing absences and ensuring appropriate cover | Legal obligation  Performance of the contract  In our legitimate interest to manage absences and ensure appropriate cover | Legal obligation/right in relation to employment | During employment and up to 6 months after employment ends |
| [Trade union membership] | [Payment of trade union subscriptions via payroll deductions; facilitating meetings with union representatives for collective bargaining purposes; compliance with legal obligations to allow time off for trade union activities, training, etc.] | [Legal obligation  In our legitimate interest to engage with trade union representatives and manage and facilitate time off, etc. for trade union representatives] | [Legal obligation/right in relation to employment] | [During employment and up to 6 months after employment ends] |
| Equal opportunities and diversity (which could include information about [your race or ethnicity, religious beliefs, sexual orientation, or health]). | To monitor equality of opportunity and diversity in our organisation, comply with company policies | In our legitimate interest to understand how our organisation is doing with regard to diversity and equal opportunities | Public interest in monitoring equal opportunities within the workforce | During employment and up to 6 months after employment ends |
| [Biometric data that is used to identify you, e.g. including finger print laptop/mobile device security or building entry systems] | [To ensure security of laptops and mobile devices/to control access to our premises] | [In our legitimate interest to maintain the security of our business premises/equipment] | [Your explicit consent (given voluntarily – if you do not consent then alternative means of access to buildings/laptops/mobile devices will be made available). If you do consent, you have the right to withdraw your consent at any time, in which case alternative means of access to buildings/laptops/mobile devices will be made available.]  [*OR if applicable:* Legal obligation/right in relation to employment  (health and safety)] | During employment and up to 6 months after employment ends |
| Criminal convictions/ offences | When you are working for us, if a criminal conviction comes to light, to investigate and assess the impact, if any, on your continued employment (see [Disciplinary policy]) | Legal obligations  Performance of the contract  In our legitimate interest to determine whether to employ individuals with criminal convictions in particular roles | You have manifestly made the information public  Establishing, exercising or defending legal claims  Detecting or preventing unlawful acts  Legal obligation/right in relation to employment | Decided on a case by case basis in accordance with the criteria set out in this Privacy Notice |
| Any special category data that is relevant when determining your working hours or arrangements | Paying you correctly  Complying with legal requirements regarding working time  Managing attendance, day to day operational management and dealing with requests to alter hours | Legal obligation  Performance of the contract  In our legitimate interest to manage working hours/ arrangements to ensure effective business operations | Legal obligation/right in relation to employment | During employment and up to 6 months after employment ends |
| Any special category data that is relevant to a disciplinary, grievance, or performance management process, or to an investigation prompted by a whistleblowing complaint. | To investigate the disciplinary or grievance issue, to manage your performance, or to investigate the whistleblowing complaint, as applicable | Legal obligations  Performance of the contract  In our legitimate interest to handle disciplinary, grievance, performance and whistleblowing matters promptly and effectively | Legal obligation/right in relation to employment  You have manifestly made the information public  Establishing, exercising or defending legal claims  Public interest in detecting or preventing unlawful acts | Decided on a case by case basis in accordance with the criteria set out in this Privacy Notice |
| Any special category data that is relevant to our strategic decision-making processes, to planning business operations, to any company restructuring or reorganisation, subject access requests by Employees, customers or others, actual and potential legal claims, corporate reporting and business risk analysis | To enable us to carry out the company business, analyse current business performance, plan for the future, restructure or reorganise, present information in reports to relevant audiences such as shareholders, respond to subject access requests as required by law, protect the company from legal claims, seek professional advice as and when required in the course of running our business | Legal obligation  Performance of the contract  In our legitimate interest to carry out the company business, including taking strategic decisions in the interest of the business, communicating about the business with relevant audiences and seeking professional advice where appropriate | Legal obligation/right in relation to employment  Establishing, exercising or defending legal claims | Decided on a case by case basis in accordance with the criteria set out in this Privacy Notice |

**More information about how we share your personal data**

|  |  |  |  |
| --- | --- | --- | --- |
| **Who we share your personal data with** | **What data we share** | **Why we share it** | **Legal ground** |
| [*If you share personal data with a parent or other group company:* Name of parent or other group company] | [*Example*:  Any of your personal data that is relevant] | [*Example*:  To make business decisions connected with your career and pay and benefits, such as [inclusion in the group-wide bonus scheme/centralised monitoring of individual performance]  To manage the company’s or group’s business  To monitor company performance  To provide system maintenance support and hosting of data] | [*Example*:  Legal obligation  Performance of the contract  In our legitimate interest to manage the business and Employee performance] |
| [*If you use any third party service providers*:  ***EITHER*** *Name of each provider* ***OR*** *description of each provider, e.g. IT support provider, payroll provider, background checks provider, travel service providers, events management partners, pension and benefits providers, etc.*] | [*Example:*  [Pay, NI and bank details / IT usage details / employment history, address / travel dates, booking requirements / *insert type of data as appropriate for relevant service provider*] | [*Example:*  [To enable the service provider to carry out [payroll functions/IT services/background checks/travel bookings/events bookings/pension and benefits administration]/ *insert purpose as appropriate for relevant service provider*] | [*Example*:  Performance of contract  In our legitimate interest to engage appropriate service providers to manage [payroll/IT/background checks/business travel arrangements/company events, etc.] |
| Our legal and other professional advisers appointed from time to time | Any of your personal data that is relevant | To obtain legal or other professional advice about matters related to you or in the course of dealing with legal disputes with you or other Employees; to obtain advice on business management and planning, including accounting advice; to independently audit our accounts | Legal obligation  Performance of contract  In our legitimate interest to seek professional advice to clarify our rights/obligations and appropriately defend ourselves from potential claims; to manage the business and its finances  (In relation to special category data – legal obligation/right in relation to employment; defending legal claims) |
| Our insurers from time to time | Any of your personal data that is relevant | To ensure appropriate levels of insurance cover for our business and to make insurance claims which concern you | Legal obligation  In our legitimate interest to maintain business insurance and make claims under it where applicable  (In relation to special category data – legal obligation/right in relation to employment; defending legal claims) |
| Occupational health professionals/medical professionals | Details of your sickness absences, information we already have about your health/medical conditions as relevant | To seek a medical report about you [in accordance with our attendance management policy]/to carry out assessments required by health and safety legislation | Legal obligation  In our legitimate interest to manage sickness, absence and health issues arising in our workforce  (In relation to special category data – Legal obligation/right in relation to employment; defending legal claims) |
| [*If you use private investigators to look into suspected abuse of sickness absence / other misconduct* In exceptional circumstances, private investigators] | [Home address, details of your absences / conduct, information we already have about your health/medical conditions as relevant] | [To enable investigation of suspected serious abuse of sickness absence, or other serious misconduct] | [Legal obligation  In our legitimate interest to prevent abuse of sickness absence or other misconduct  (In relation to special category data – Legal obligation/right in relation to employment; defending legal claims)] |
| [*List relevant legal authorities and regulators*:  HMRC  Home Office  [Public Health England]  [*Name others*] | Pay, tax and NI details  Name, date of birth, nationality and other requested details  [Covid-19 test results]  [*insert type of personal data as relevant for each regulator*] | To comply with regulatory and legal obligations  If requested in the context of immigration control  [To comply with public health guidance] | Legal obligation  In our legitimate interest to comply with requests from Government agencies relating to immigration control  [In our legitimate interest to comply with applicable public health guidance]  (In relation to special category data – Legal obligation/right in relation to employment or social security; defending legal claims[; processing is necessary in the public interest in the area of public health]) |
| [Trade unions] | [Name, union membership, check-off details [*insert any additional personal data shared with union*]] | [To facilitate good industrial relations with [recognised] trade union]  [To facilitate check-off arrangements for union subscription payments]  [To facilitate time off for union representatives] | [In our legitimate interest to maintain good relations with [recognised] trade union]  [(In relation to special category data – legal right/obligation in relation to employment; you have manifestly made the information public)] |
| Potential purchasers/new service providers | Any of your personal data that is relevant | To provide relevant information to prospective purchasers or new service providers in the event of a possible business transfer, a business or share sale, takeover or other corporate transaction | Legal obligation  In our legitimate interest to consider/proceed with a transfer/sale of the business and information is required by prospective purchasers |
| Customers, potential customers, shareholders and interested parties | Any of your personal data that is relevant, including in particular business contact details, information about role and experience | Inclusion in corporate reports, for use in business communications, to obtain security clearance to work on customers’ premises | Legal obligation  In our legitimate interest to communicate about the business and our Employees to appropriate audiences, which include customers, potential customers, shareholders and other interested parties |
| Third parties at your request | Employment details as relevant | At your request, to provide a reference to a potential new employer/details of your employment to a mortgage company | In our legitimate interest/that of the third party recipient to action reasonable requests by you to provide your personal data to third parties  [With your consent] |
| An individual (e.g. another Employee or a customer) who has made a subject access request under data protection law | Only such of your personal data as is relevant to the individual’s request and we are required by law to disclose | To comply with our legal obligation to respond to a subject access request | Legal obligation  In our legitimate interest to respond promptly and properly to subject access requests  (In relation to special category data – legal obligation/right in relation to employment; defending legal claims) |