

**Privacy Notice - employees, workers, contractors and partners**

**WHAT IS THE PURPOSE OF THIS DOCUMENT?**

Howes Percival LLP (“the Firm” or “we”) is committed to protecting the privacy and security of your personal data.

This privacy notice describes how we collect and use personal data about you during and after your working relationship with us, in accordance with UK data protection law, including the Data Protection Act 2018 and the EU retained law version of the General Data Protection Regulation 2016 (UK GDPR).

This privacy notice applies to all employees, workers, contractors and partners/members. It does not form part of any contract of employment or engagement. We may vary, amend, alter or replace this privacy notice at any time.

The Firm is a “data controller”. This means that we are responsible for deciding how we hold and use personal data about you. We are required under the UK GDPR to notify you of the information contained in this privacy notice.

**DATA PROTECTION PRINCIPLES**

We will comply with data protection law and principles, which means that your personal data will be:

1. Used lawfully, fairly and in a transparent way.
2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
3. Relevant to the purposes we have told you about and limited only to those purposes.
4. Accurate and kept up to date.
5. Kept only as long as necessary for the purposes we have told you about.
6. Kept securely.

**THE KIND OF PERSONAL DATA WE HOLD ABOUT YOU**

“Personal data” means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

There are “special categories” of more sensitive personal data which require a higher level of protection.

 We will collect, store, and use the following categories of personal data about you:

1. Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
2. Date of birth.
3. Gender.
4. Marital status and dependants.
5. Next of kin and emergency contact information.
6. National Insurance number.
7. Bank account details, payroll records and tax status information.
8. Salary, annual leave, pension and benefits information.
9. Start date.
10. Location of employment or workplace.
11. Copy of driving licence if you are on our business insurance policy.
12. Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process).
13. Employment records (including job titles, work history, working hours, training records and professional memberships).
14. Copies of certificates relating to professional qualifications.
15. Compensation history.
16. Performance information.
17. Disciplinary and grievance information.
18. CCTV footage (at our Northampton and Norwich offices) and other information obtained through electronic means such as building alarm access records.
19. Information about your use of our information and communications systems.
20. Photographs.

We may also collect, store and use the following “special categories” of more sensitive personal data:

1. Information about your race or ethnicity, religious beliefs, sexual orientation, political opinions and trade union membership.
2. Information about your health, including any medical condition, health and sickness records.
3. Information about criminal convictions and offences.

**HOW IS YOUR PERSONAL DATA COLLECTED?**

We collect personal data about employees, workers, contactors and partners/members through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may collect additional information from third parties including former employers (information will only be collected from former employers in relation to reference checks and you will have consented to these checks by providing us with details of your chosen referees). If you are a solicitor, we will check the Solicitors Regulation Authority (SRA) website to ensure that you a solicitor and check that you have a practising certificate free from restrictions. We may also have to obtain personal data relating to criminal offences or convictions from you (see: Information about Criminal Convictions below).

We will also carry out the following checks at the commencement of employment, or during the course of your employment with the Firm:

1. Electronic verification checks on new joiners (currently carried out via Smartsearch), to confirm your identity including (if applicable) right to work in the UK. Electronic verification checks are repeated annually during your employment.
2. SRA section 43 restrictions check on all new joiners, and repeated annually.
3. DBS checks on all new partners including salaried partners.
4. Adverse media checks on all new starters, carried out via Google, and repeated annually for all partners and staff.

We will collect additional personal data in the course of job-related activities throughout the period of your employment for us.

**HOW WE WILL USE INFORMATION ABOUT YOU** **GENERALLY**

We will only use your personal data when the law allows us to. Most commonly, we will use your personal data in the following circumstances:

1. Where we need to perform the contract we have entered into with you.

2. Where we need to comply with a legal or regulatory obligation.

3. 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.

We may also use your personal data in the following situations, which are likely to be rare:

1. Where we need to protect your interests (or someone else’s interests).

2. Where it is needed in the public interest or for official purposes.

**HOW WE USE PARTICULARLY SENSITIVE PERSONAL DATA**

”Special categories” of particularly sensitive personal data require higher levels of protection. This includes the following information: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic/biometric data, health, sex life or sexual orientation.

We need to have further justification for collecting, storing and using this type of personal data. We may process special categories of personal data in the following circumstances:

1. In limited circumstances, with your explicit written consent;
2. Where it is necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law and in line with our data protection policy;
3. Where it is needed in the public interest, such as for equal opportunities monitoring, and in line with our data protection policy.
4. Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.

Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your vital interests (or someone else’s interests) and you are not capable of giving your consent, or where you have already made the information public.

**SITUATIONS IN WHICH WE WILL USE YOUR PERSONAL DATA**

We need all the categories of information in the list above (see; [*the kind of information we hold about you*](#co_anchor_a486023_1)) primarily to allow us to perform our contract with you (we reference this below with a “\*”) and to enable us to comply with legal obligations (we reference this below with a “\*\*”). In some cases we may use your personal data to pursue legitimate interests of our own or those of third parties (we reference this below with a “\*\*\*”), provided your interests and fundamental rights do not override those interests.

The situations in which we will process your personal data are listed below. We have indicated by asterisks the purpose or purposes for which we are processing or will process your personal data as explained above, as well as indicating which categories of data are involved. Where sensitive personal data may be indicated, we also indicate which legal basis or bases we are relying on for processing that information.

|  |  |
| --- | --- |
| **Purpose** | **Legal Basis** |
| Making a decision about your recruitment or appointment, which will include obtaining references from your referees. | \* and \*\*\* |
| Determining the terms on which you work for us. | \* and \*\*\* |
| Checking you are legally entitled to work in the UK. | \*\* (and where this amounts to sensitive personal data, to ensure we are complying with employment, social security or social protection laws) |
| For future trainee solicitors, in dealing with funding arrangements for LPC and GDL (or equivalent). | \* |
| Paying you, which will include obtaining bank account details from you, inputting information into Sage (our payroll system), our HR database (Sage HR) and providing information to HMRC or reimbursing expenses to you. We also use Thrive for our Learning Management System. For supporting with health conditions, we use Medigold Health and Gipping Ltd to obtain occupational health reports. We also use Fortis Therapy to support our staff.  | \* |
| If you are an employee, deducting tax and National Insurance contributions. | \* and \*\* |
| Administering salary sacrifice arrangements for employees. | \* |
| Providing the following benefits to you if you are an employee:1. Pension (Scottish Widows)
2. Private health insurance (Aviva)
3. Permanent health insurance (AIG)
4. Employee Assistance Programme (AIG)
5. Life insurance – (Legal & General)
6. Childcare vouchers (Computershare)
7. Health Cash Plan (Medicash)
8. Dental Insurance (UNUM)
9. Cycle to Work Scheme (Cyclescheme)
10. Holiday buy and sell
11. Online discount shopping portal (PERKS AT WORK)
12. Electric Car Scheme (ECS)
 | \* |
| If you are a partner (and in some cases for consultants) for arranging the following benefits:1. Permanent health insurance (Aviva )
2. Partners Group Life Assurance - (Legal & General)
3. BUPAHealth Checks – (Every 2 years)
4. Employee Assistance Programme (AIG)
5. Critical illness (Aviva)
6. Administering your car account and mileage expenses
7. Online discount shopping portal (PERKS AT WORK)
8. Electric Car Scheme (ECS)
 | \* and \*\*\* |
| Liaising with Mattioli Woods and Zest who are our employee benefits and pensions consultants and with whom we have our on line HP Flex platform (which is provided by Zest) in terms of providing you with employee benefits and for administering HP flex, including Perks at Work for the on line discount shopping portal) and to provide you with the above benefits, together with critical illness for employees, with Aviva. | \* |
| Administering the contract we have entered into with you. | \* |
| In relation to partners, in dealing with rights and obligations under the LLP Deed. | \* |
| Business management and planning, including accounting and auditing. | \*\*\* |
| For financial purposes, including time recording, processing information relating to utilisation, recovery rates, WIP, billing, charge out rates, cost rates, budgets, targets, aged debts and other financial information for business purposes and in providing cost rates and information about fees to clients. | \*\*\* |
| Conducting performance reviews, annual appraisals, and mid-year appraisals, managing performance and determining performance requirements. | \* and \*\*\* (and in such cases and where this amounts to sensitive information, to comply with relevant employment, social security and social protection laws). |
| Making decisions about salary reviews and compensation (including any bonuses reviews). | \*, \*\* and \*\*\* |
| Assessing qualifications, experience or suitability for a particular job or task, including decisions about promotions. | \*\*\* |
| Gathering evidence for possible grievance or disciplinary hearings and holding possible grievance and disciplinary hearings including any appeals. | \*\* and \*\*\* (and where this involves the use of sensitive personal data, to comply with employment, social security and social protection laws) |
| Dealing with other absences and leave, for example, maternity, paternity, parental leave, shared parental leave, adoption leave, career breaks, emergency dependents leave, bereavement leave and any other leave that may be requested. | \*, \*\* and \*\*\* (and where involving sensitive personal data, complying with employment laws) |
| Dealing with any flexible working requests and other requests to change hours. | \*, \*\* and \*\*\* (and where dealing with sensitive personal data, to comply with employment laws) |
| Addressing other HR issues that may arise, including responding to any informal complaints, in investigating any whistle-blowing complaints. | \*, \*\* and \*\*\* (and where dealing with sensitive personal data, complying with employment law obligations) |
| Making decisions about your continued employment or engagement. | \*\*\* (and where dealing with sensitive personal data, complying with employment law obligations) |
| Making arrangements for the termination of our working relationship. | \*\*\* |
| Education, training and development requirements. | \*\* and \*\*\* |
| Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work. | \*\* and \*\*\* |
| Ascertaining your fitness to work and consideration of any reasonable adjustments. | \*\* and \*\*\* (and where involving sensitive personal data to comply with employment laws and/or to assess your working capacity pursuant to a contract with a health professional) |
| Managing sickness absence and making claims against a relevant insurance policy (income protection/permanent health insurance and the like). | \*, \*\* and \*\*\* (and where involving sensitive personal data to comply with employment laws and/or to assess your working capacity pursuant to a contract with a health professional) |
| Complying with health and safety obligations. | \*\* (and if involving sensitive personal data, to comply with employment laws) |
| To prevent fraud. | \*\* and \*\*\* |
| To monitor your use of our information and communication systems to ensure compliance with our IT policies. | \*\*\* (and if involving sensitive personal data, to comply with employment laws) |
| To monitor access to our buildings for security purposes via alarm access codes and CCTV, which ensures the security of our business and the safety of our employees and visitors, and to detect and prevent crime. We only have CCTV in operation in the Northampton and Norwich offices.At our Northampton office; we have one camera that covers the entrance to our car park, giving a view of the barrier arm, key pad and intercom, the other covers the front entrance to our building and an area of the car park which is part of our demise. The images from both cameras are only viewable from behind our reception desk.At our Norwich office the CCTV monitors the main reception entrance (inner and outer doors), the entrance to the car park and the alleyway from the car park to the main road. It primarily covers those visiting our offices (but is angled so as not to cover members of the public walking by) and cars entering our car park.Images from cameras can be viewed from the reception desk at the relevant office and in secure setting by authorised personal for a short period after (save if there is a legal basis for keeping footage long, such as in the event of a criminal investigation). | \*\*\* |
| To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution. | \*\* and \*\*\* |
| For providing relevant information to clients and prospective clients and intermediaries for business purposes which may include your work email addresses and contact numbers, providing your relevant qualifications, credentials and experience to them and photographs for marketing materials to clients, on our website and on the intranet and ensuring the smooth conduct of the matter. | \*\*\* |
| For processing information as required under our Government contracts. | \*\* and \*\*\* |
| For business development purposes in monitoring your activity, pipeline, targets and supporting you to convert those targets into clients. | \*\*\* |
| To conduct data analytics studies to review and better understand employee retention and attrition rates. | \*\*\* |
| Equal opportunities monitoring.  | \*\* and \*\*\* (and to comply with employment laws and/or for reasons that are in the public interest) |
| To comply with our regulatory obligations with the SRA, which will include applying for practicing certificates, ensuring that you have completed any necessary continuing personal development, processing of information by the COLP and COFA, investigations by the COLP and COFA, making notifications of potential breaches/material breaches to the SRA and carrying out any investigations required by the SRA, and for trainee solicitors in registering your training contract with the SRA, completing a certificate of fitness, ensuring that we are complying with our training obligations and signing off your training contract as having been satisfactorily completed and for dealing with issues relating to the SRA Assessment of Character and Suitability Rules. | \*\* and \*\*\* |
| If you indicate a possible claim against the firm or there is another notifiable event, we will need to disclose your details and details of that potential claim to our insurers (under our employee liability/employment practices insurance). Generally, it will be a partner responsible for managing the claim/matter who will disclose details to our broker, currently Hugh J Boswell Limited of Carrow Hill, Norwich and with our insurer, Travellers Insurance Company Limited, Exchequer Court, 33 St Mary Axe, London,EC3A 8AG. | \*\*\* |
| For insurance purposes in relation to renewal and notification of claims. In this respect:1. Our insurance broker is Howden Insurance Brokers Limited.
2. Our current PI insurers for the primary layer (up to £5m) are Aviva Insurance Limited, and QBE UK Limited D1806.
3. Our first excess layer insurers are Markel International Insurance Company Limited, Starr International (Europe) Limited, Lloyd’s Syndicate CNP 4444, Lloyd’s Syndicate HDU 382 and Axis Specialty Europe SE.
4. The next excess layer insurers are Great Lakes Insurance SE, HCC International Insurance Company PLC, Liberty Mutual Insurance Europe SE and Chubb European Group SE.
5. The next excess layer insurers are Markel International Insurance Company Limited, XL Caitlin Insurance Company UK Limited, Allied World Assurance Company (Europe) dac, Chubb European SE, Great Lakes Insurance SE, Lloyd’s Syndicate CNP 4444, Lloyd’s Syndicate ASC 1414 and Lloyd’s Syndicate AUL 1274.
6. The next excess layer insurers are Swiss Re International SE, Great Lakes Insurance SE, Liberty Mutual Insurance Europe SE, Scor UK Company Limited, Lloyd’s Syndicate AUL 1274, Lloyd’s Syndicate AUW 609, Lloyd’s Syndicate PBS 1492, Lloyd’s Syndicate TAL 1183, Lloyd’s Syndicate FDY 435 and Lloyd’s Syndicate CNP 4444.
7. We have Management liability insurance with HCC International Insurance Company PLC.
8. The information that we give insurers is as follows:
9. Insurance renewal – data about the firm to include all/any information that may influence the provision of insurance and the level of the premium, for example, number of offices, turnover, number of staff, claims history, material acquisitions/hires, names of partners, criminal convictions etc. This information is used to seek/secure insurance; and
10. Notification of claims – client details (or staff details where the notification relates to the management liability insurance), details of matter, details of circumstance/claim being notified. The insurers assess this information and take a view on merits and potential loss and keep an internal record. They will also make payment under our policy where appropriate. If necessary, they will use this information to instruct one of their panel firms to act on our behalf in defending a claim.
 | \*\*\* |
| For the purposes of our obligations/contract with the Lender Exchange in relation to residential conveyancing. This requires the firm’s data to be uploaded to a portal which lenders in the scheme can access. The Lender Exchange requires us to provide information on all partners of the firm and all solicitors that carry out residential conveyancing. <https://www.lenderexchange.co.uk/> They request ID and practising certificates to be submitted and the following information: Name; Date of birth; Home address and if you have lived there less than 3 years your previous address; Email address; Qualification date; Place of birth; Nationality; Previous employment history; Whether you will carry out conveyancing? If so, number of years’ experience; Whether you are a director/investor/shareholder of another company; Any adverse credit in the last 6 years; Whether you are subject to a current regulatory body investigation; whether you have any restrictions on your practising certificate; whether you or any practice whilst you were a partner, member, director, or employee, have been the subject of an intervention or any disciplinary action by a regulator of legal profession in the jurisdiction in which you operated; whether you are a CoT signatory; whether any of your previous firms whilst you were working there ever been removed or rejected from any Lender’s Conveyancing Panel. Once this info is submitted to the lender exchange the individual receives an email and link to authorise submission. | \*\*\* |

In addition to the above which on occasions may include the processing of sensitive personal data, we will also use your sensitive personal data in the following ways:

1. We will use information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws.
2. We will use information regarding protected characteristics under the Equality Act 2010 (sex, age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief) to ensure that we do not discriminate against you and/or to protect you from discrimination or harassment or to otherwise comply with our obligations under the Equality Act 2010 and other employment laws.
3. We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to assess reasonable adjustments that may be needed in any recruitment process, to monitor and manage sickness absence and to administer benefits and to ensure that we do not discriminate against you.
4. We will use information about your race or national or ethnic origin, religious, philosophical or moral beliefs, or your sexual life or sexual orientation, to ensure meaningful equal opportunity monitoring and reporting.

We may use information about any trade union membership if we are required to pay any trade union premiums and/or to comply with employment law obligations.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal data and sensitive personal data.

**If you fail to provide personal data**

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers). We will let you know if this is the case.

**Change of purpose**

We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

**DO WE NEED YOUR CONSENT?**

We do not need your consent if we use special categories of your personal data in accordance with our written policy to carry out our legal obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the specific information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

**INFORMATION ABOUT CRIMINAL CONVICTIONS**

The Firm is subject to the SRA Principles 2019 (SRA Principles) and the SRA Code of Conduct for Firms 2019 (the Code for Firms) and are entitled to make enquiries about criminal offences and convictions to ensure that the Firm employs suitable people at all levels of the Firm.

We may only collect and use information relating to criminal convictions, if it is appropriate given the nature of your role and where the law allows us to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of your employment. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our data protection policy.

We would only process information relating to criminal offences and convictions if you or the SRA disclosed to us a criminal offence or conviction which is relevant to your role and suitability to practice. In this event, we will discuss this with you and process this information if we consider that it effects your suitability for the role and/or places us in breach of a legal obligation and/or is relevant to your role or the duties that you perform.

Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else’s interests) and you are not capable of giving your consent, or where you have already made the information public.

New employees may be required to complete a Baseline Personal Standard Security form, which contains a criminal conviction declaration form. It is a condition of our Government contracts that all new employees who will or may undertake government work complete this form. As part of these contracts, we may have continuing obligations to provide them with any information that we become aware of relating to criminal convictions and bankruptcy of partners.

We are allowed to use your personal data in this way to perform your contract of employment, as part of our legitimate interests as a regulated firm of solicitors and to carry out our legal obligations (in particular employment law obligations for employing persons to work in a regulated firm of solicitors). When we collect criminal offence data this will be kept securely and restricted only to those persons involved decision-making regarding your employment or suitability for the role and/or when required by our regulators.

**AUTOMATED DECISION-MAKING**

Automated decision-making takes place when an electronic system uses personal data to make a decision without human intervention. We are allowed to use automated decision-making in the following circumstances:

1. Where we have notified you of the decision and given you 21 days to request a re-consideration.

2. Where it is necessary to perform the contract with you and appropriate measures are in place to safeguard your rights.

3. In limited circumstances, with your explicit written consent and where appropriate measures are in place to safeguard your rights.

If we make an automated decision on the basis of any particularly sensitive personal data, we must have either your explicit written consent or it must be justified in the public interest, and we must also put in place appropriate measures to safeguard your rights.

You will not be subject to decisions that will have a significant impact on you based solely on automated decision-making, unless we have a lawful basis for doing so and we have notified you.

We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

**DATA SHARING**

We may have to share your data with third parties, including third-party service providers and other entities in the group. We have provided a list of those third parties in this notice (see: *Situations in which we will use your personal data*). The relevant third parties may be subject to change from time to time, and we will endeavour to keep this list up-to-date but if you have any specific concerns or want to confirm the current providers please contact us.

We require third parties to respect the security of your data and to treat it in accordance with the law.

We may transfer your personal data outside the UK and European Economic Area but if we do so we will seek to comply with our data protection policy (see: *Transferring Information outside the European Economic Area*).

If we do, you can expect a similar degree of protection in respect of your personal data.

**Why might you share my personal data with third parties?**

We will share your personal data with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

**Which third-party service providers process my personal data?**

”Third parties” includes third-party service providers (including contractors and designated agents) and other entities within our group. The following activities are carried out by third-party service providers: payroll (this is Sage), pension administration, benefits provision and administration (this is Mattioli Woods and Zest) and the benefits providers referred to above), IT and archiving services (including Mimecast, Tessian, Wardle Keach, Oasis/Iron Mountain etc.), our internet providers, Grandad, our PR providers (Gordon Maw) and our insurance providers and brokers (see: *Situations in which we will use your personal data*).

**How secure is my information with third-party service providers and other entities in our group?**

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal data in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

**What about other third parties?**

We may share your personal data with other third parties, for example in the context of the possible sale or restructuring of the business. We may also need to share your personal data with a regulator or to otherwise comply with the law.

**Transferring information outside the UK or European Economic Area (“EEA”)**

We do not envisage transferring your data outside of the UK or EEA, save that it may from time to time be necessary to transfer some of your details to clients and prospects outside of the UK or EEA (such as business contact details, name, telephone number, email address, qualifications and specialisms etc.).

Mattioli Woods and Zest, who currently support us with our employee benefits consulting and on line platform have informed us that, it is possible that they may transfer personal data outside of the UK/EEA. Where this is necessary, they will ensuring that measures are in place, as required by UK data protection laws, to ensure that privacy rights are guaranteed.

**DATA SECURITY**

We have put in place measures to protect the security of your information.

A summary of our security measures are set out within our data protection policy, a copy of which will be on our intranet or can be obtained on request from the People Team.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so. Details of our data breach policy are set out in our data protection policy.

**DATA RETENTION**

**How long will you use my personal data for?**

We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Details of retention periods for different aspects of your personal data are available in our retention policy and schedule which is on our intranet and which is available from the People Team.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements. We also take into account the limitation periods applicable for making any claims against us which features in our decision-making on retention.

In some circumstances we may anonymise your personal data so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, worker, contractor or partner of the Firm we will retain and securely destroy your personal data in accordance with our data retention policy and schedule.

**RIGHTS OF ACCESS, CORRECTION, ERASURE, AND RESTRICTION**

**Your duty to inform us of changes**

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your working relationship with us.

**Your rights in connection with personal data**

Under certain circumstances, by law you have the right to:

1. **Request access** to your personal data (commonly known as a “data subject access request”). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.
2. **Request correction** of the personal data that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected. Please note that we may need to verify the accuracy of the new personal data that you provide.
3. **Request erasure** of your personal data. This enables you to ask us to delete or remove personal data 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). Please note, however, that we may not always be able to comply with your request for specific legal reasons which will be notified to you, if applicable, at the time of your request.
4. **Object to processing** of your personal data where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases we may demonstrate that we have compelling legitimate grounds to process your personal data which override your rights and freedoms.
5. **Request the restriction of processing** of your personal data in certain circumstances. 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. **Request the transfer** of your personal data to you or to another party. This right only applies to automated information for which you initially provided consent for us to use, or where we used the information to perform a contract with you.

If you want to review, verify, correct or request erasure of your personal data, object to the processing of your personal data, or request that we transfer a copy of your personal data to you or another party, please contact the Head of People in writing.

**No fee usually required**

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request for access is clearly unfounded or excessive. Alternatively, we may refuse to comply with the request in such circumstances.

**What we may need from you**

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal data is not disclosed to any person who has no right to receive it.

**RIGHT TO WITHDRAW CONSENT**

In the limited circumstances where we have relied on your consent to the collection, processing and transfer of your personal data for a specific purpose (which will be rare); you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Head of People. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

**DATA PROTECTION OFFICER**

We have appointed James Howarth, Partner, as our data protection officer (DPO) to oversee compliance with this privacy notice. If you have any questions about this privacy notice or how we handle your personal data, please contact the DPO. You have the right to make a complaint at any time to the Information Commissioner’s Office (ICO), the UK supervisory authority for data protection issues.

**CHANGES TO THIS PRIVACY NOTICE**

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal data.

*The Firm’s Data Protection Officer is responsible for this Notice which was adopted on 8 May 2018 and last revised on 22 January 2024.*