Rödl & Partner

PRIVACY NOTICE

1 Overview

1.1 The Company takes the security and privacy of your data seriously. We need to gather and use information or 'data' about you as part of our business and to manage our relationship with you. We intend to comply with our legal obligations under the **Data Protection Act 2018** (the '2018 Act') and the **EU General Data Protection Regulation** ('GDPR') in respect of data privacy and security. We have a duty to notify you of the information contained in this policy.

1.2 This policy applies to current and former employees, workers, volunteers, apprentices, interns and consultants. If you fall into one of these categories then you are a 'data subject' for the purposes of this policy. You should read this policy alongside your contract of employment (or contract for services) and any other notice we issue to you from time to time in relation to your data.

1.3 The Company has separate policies and privacy notices in place in respect of job applicants, customers, suppliers and other categories of data subject. A copy of these can be obtained from the Practice Team.

1.4 The Company has measures in place to protect the security of your data in accordance with our Data Protection Policy, which can be found on the U:\Internal\Company Policies or obtained from the Practice Team.

1.5 The company will hold data in accordance with our Data Retention Policy which can be found in U:\Internal\Company Policies or obtained from the Practice Team. We will only hold data for as long as necessary for the purposes for which we collected it.

1.6 The Company is a '**data controller**' for the purposes of your personal data. This means that we determine the purpose and means of the processing of your personal data.

1.7 This policy explains how the Company will hold and process your information. It explains your rights as a data subject. It also explains your obligations when obtaining, handling, processing or storing personal data of any nature in the course of working for, or on behalf of, the Company.

1.8 This policy does not form part of your contract of employment [or contract for services if relevant] and can be amended by the Company at any time. It is intended that this policy is fully compliant with the 2018 Act and the GDPR. If any conflict arises between those laws and this policy, the Company intends to comply with the 2018 Act and the GDPR.

2 Data Protection Principles

2.1 Personal data must be processed in accordance with six '**Data Protection Principles**.' It must:

- be processed fairly, lawfully and transparently;
- be collected and processed only for specified, explicit and legitimate purposes;
- be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- be accurate and kept up to date. Any inaccurate data must be deleted or rectified without delay;

- not be kept for longer than is necessary for the purposes for which it is processed; and
- be processed securely.

We are accountable for these principles and must be able to show that we are compliant.

3 How we define personal data

3.1 '**Personal data**' means information which relates to a living person who can be **identified** from that data (a '**data subject**') on its own, or when taken together with other information which is likely to come into our possession. It includes any expression of opinion about the person and an indication of the intentions of us or others, in respect of that person. It does not include anonymised data.

3.2 This policy applies to all personal data whether it is stored electronically, on paper or on other materials.

3.3 This personal data might be provided to us by you, for example from forms completed by you at the start of or during your employment [such as new starter forms or benefit forms]. In some cases, we may collect personal data about you from someone else such as [references from a former employer, information from your doctor with your consent], [or information from criminal records checks permitted by law]. Also, it could be created by us from correspondence with you or through interviews, meetings or other assessments.

3.4 It could be provided or created during the recruitment process or during the course of the contract of employment [or services] or after its termination. It could be created by your manager or other colleagues.

3.5 We will collect and use the following types of personal data about you:

- recruitment information such as your application form and CV, giving details of your qualifications, skills, experience and employment history with start and end dates; references, qualifications and membership of any professional bodies and details of any pre-employment assessments
- your name, address and contact details including email address and telephone numbers, date of birth and gender
- the contact details for your emergency contacts
- your marital status and family details including next of kin and dependants
- information about your contract of employment [or services] including start and end dates of employment, role and location, days of work and working hours, details of promotion, salary (including details of previous remuneration), pension, benefits and holiday entitlement
- your bank details and information in relation to your tax status including your national insurance number
- your identification documents including passport and driving licence and information in relation to your immigration status and right to work for us
- details of periods of leave taken by you including holidays, sickness absence, family leave, [sabbaticals] and the reasons for the leave
- information relating to disciplinary or grievance investigations and proceedings involving you (whether or not you were the main subject of those proceedings)
- information relating to your performance and behaviour at work
- training records
- electronic information in relation to your use of IT systems/swipe cards/telephone systems
- your images (whether captured on CCTV, by photograph or video)
- any other category of personal data which we may notify you of from time to time.

4 How we define special categories of personal data

4.1 '**Special categories of personal data**' or sensitive personal data are types of personal data consisting of information as to:

- your racial or ethnic origin;
- your political opinions;
- your religious or philosophical beliefs;
- your trade union membership;
- your genetic or biometric data;
- your health;
- your sex life and sexual orientation; and
- any criminal convictions and offences.

We may hold and use any of these special categories of your personal data in accordance with the law.

5 How we define processing

5.1 **'Processing'** means any operation which is performed on personal data such as:

- collection, recording, organisation, structuring or storage;
- adaption or alteration;
- retrieval, consultation or use;
- disclosure by transmission, dissemination or otherwise making available;
- alignment or combination; and
- restriction, destruction or erasure.

This includes processing personal data which forms part of a filing system and any automated processing.

6 How will we process your personal data?

6.1 The Company will process your personal data (including special categories of personal data) in accordance with our obligations under the 2018 Act.

6.2 We will use your personal data for:

- performing the contract of employment (or services) between us
- complying with any legal obligation
- if it is necessary for our legitimate interests (or for the legitimate interests of someone else). However, we can only do this if your interests and rights do not override ours (or theirs).
- You have the right to challenge our legitimate interests and request that we stop this processing. See details of your Data Subject Rights in section 15 below.

We can process your personal data for these purposes without your knowledge or consent. We will not use your personal data for an unrelated purpose without telling you about it and the legal basis that we intend to rely on for processing it.

7 Data Impact Assessments

7.1 Some of the processing that we carry out may result in risks to privacy. Where processing would result in a high risk to individual's rights and freedoms, we will carry out a data protection impact assessment to determine the necessity and proportionality of processing. This will include considering the purposes for which the activity is carried out, the risks for individuals and the measures that can be put in place to mitigate those risks.

8 What if you do not provide personal data?

8.1 If you choose not to provide us with certain personal data you should be aware that we may not be able to carry out certain parts of the contract between us. For example, if you do not provide us with your bank account details we may not be able to pay you. It might also stop us from complying with certain legal obligations and duties which we have such as to pay the right amount of tax to HMRC or to make reasonable adjustments in relation to any disability you may suffer from.

8.2 You may also have to provide us with data such as in relation to statutory leave entitlements. Failing to provide the data may mean you are unable to exercise your statutory rights.

8.3 If you do not provide other information, for example information about absence, disciplinary or other matters under the implied duty of good faith, this will hinder our ability to administer the rights and obligations arising as a result of the employment relationship efficiently.

9 Examples of when we might process your personal data

9.1 We have to process your personal data in various situations during your recruitment, employment [or engagement] and even following termination of your employment [or engagement].

9.2 For example (and see section 9.6 below for the meaning of the asterisks):

- to decide whether to employ (or engage) you
- to decide how much to pay you, and the other terms of your contract with us
- to check you have the legal right to work for us
- to carry out the contract between us including where relevant, its termination
- to operate and keep a record of other types of leave (including maternity, adoption, parental, paternity and shared parental leave*)
- training you and reviewing your performance*
- to decide whether to promote you
- to decide whether and how to manage your performance, absence or conduct*
- to carry out a disciplinary or grievance investigation or procedure in relation to you or someone else
- to determine whether we need to make reasonable adjustments to your workplace or role because of your disability*
- to monitor diversity and equal opportunities*
- to monitor and protect the security (including network security) of the Company, of you, our other staff, customers and others
- to monitor and protect the health and safety of you, our other staff, customers and third parties*

- to pay you and provide pension and other benefits in accordance with the contract between us*
- paying tax and national insurance
- to provide a reference upon request from another employer
- to pay trade union subscriptions*
- monitoring compliance by you, us and others with our policies and our contractual obligations*
- to comply with employment law, immigration law, health and safety law, tax law and other laws which affect us*
- to comply with the requirements of any regulatory bodies
- to answer questions from insurers in respect of any insurance policies which relate to you*
- running our business, development of our brand and planning for the future
- the prevention and detection of fraud, theft or other criminal offences
- to defend the Company in respect of any investigation or litigation and to comply with any court or tribunal orders for disclosure*
- for any other reason which we may notify you of from time to time.

9.3 We will only process special categories of your personal data (see above) in certain situations in accordance with the law. For example, we can do so if we have your explicit consent. If we asked for your consent to process a special category of personal data then we would explain the reasons for our request. You do not need to consent and can withdraw consent later if you choose by contacting the Practice Team.

9.4 We do not need your consent to process special categories of your personal data when we are processing it for the following purposes, which we may do:

- where it is necessary for carrying out rights and obligations under employment law
- where it is necessary to protect your vital interests or those of another person where you/they are physically or legally incapable of giving consent
- where you have made the data public
- where processing is necessary for the establishment, exercise or defence of legal claims
- where processing is necessary for the purposes of occupational medicine or for the assessment of your working capacity.

9.5 We might process special categories of your personal data for the purposes in paragraph 9.2 above which have an asterisk beside them. In particular, we will use information in relation to:

- your race, ethnic origin, religion, sexual orientation or gender to monitor equal opportunities
- your sickness absence, health and medical conditions to monitor your absence, assess your fitness for work, to pay you benefits, to comply with our legal obligations under employment law including to make reasonable adjustments and to look after your health and safety
- your trade union membership to pay any subscriptions and to comply with our legal obligations in respect of trade union members.

9.6 We do not take automated decisions about you using your personal data or use profiling in relation to you.

10 Sharing your personal data

10.1 Your information may be shared internally, including with members of the HR and recruitment team (including payroll), your line manager, managers in the business area in which you work and IT staff if access is necessary for the performance of their roles.

10.2 Sometimes we might share your personal data with other group companies or our contractors and agents to carry out our obligations under our contract with you or for our legitimate interests.

10.3 We require those companies to keep your personal data confidential and secure and to protect it in accordance with the law and our policies. They are only permitted to process your data for the lawful purpose for which it has been shared and in accordance with our instructions.

10.4 The legitimate activities which third parties do include:

- 'Name of company' for the processing of payroll
- 'Name of company(s)' for the provision of benefits
- 'Name of company' for the provision of occupational health services
- Previous employers for the provision of references
- 'Name of company' for employment background checks
- Disclosure & Barring Service for necessary criminal record checks

10.5 We do not send your personal data outside the European Economic Area. If this changes you will be notified of this and the protections which are in place to protect the security of your data will be explained.

11 How long do we keep personal data?

11.1 The Company will hold your personal data for periods set out in our Data Retention Policy.

12 How should you process personal data for the Company?

12.1 Everyone who works for, or on behalf of, the Company has some responsibility for ensuring data is collected, stored and handled appropriately, in line with this policy and the Company's Data Protection and Data Retention policies.

12.2 The Company's Data Protection Officer is Paul Williamson is responsible for reviewing this policy and ensuring the Company data responsibilities are met and any risks in relation to the processing of data are addressed. You should direct any questions in relation to this policy or data protection to this person.

12.3 You should only access personal data covered by this policy and of customers, suppliers as set out in Privacy Notices U:Drive - Internal\ Company Policies if you need it for the work you do for, or on behalf of, the Company and only if you are authorised to do so. You should only use the data for the specified lawful purpose for which it was obtained.

12.4 You should not share personal data informally.

12.5 You should keep personal data secure and not share it with unauthorised people.

12.6 You should regularly review and update personal data which you have to deal with for work. This includes telling us if your own contact details change.

12.7 You should not make unnecessary copies of personal data and should keep and dispose of any copies securely.

12.8 You should use strong passwords.

12.9 You should lock your computer screens when not at your desk.

12.10 Personal data should be encrypted before being transferred electronically to authorised external contacts.

12.11 Consider anonymising data or using separate keys/codes so that the data subject cannot be identified.

12.12 Do not save personal data to your own personal computers or other devices.

12.13 Ensure that personal data is saved to as few places as possible for example once appropriate personal data has been saved in the personnel folder/digital folder it should be deleted from emails and other folders.

12.14 Personal data should never be transferred outside the European Economic Area except in compliance with the law and authorisation of the Data Protection Officer Paul Williamson.

12.15 You should lock drawers and filing cabinets. Do not leave paper with personal data lying about.

12.16 You should not take personal data away from Company's premises without authorisation from your line manager or Data Protection Officer.

12.17 Personal data should be shredded and disposed of securely when you have finished with it.

12.18 You should ask for help from Data Protection Officer Paul Williamson if you are unsure about data protection or if you notice any areas of data protection or security we can improve upon.

12.19 Any deliberate or negligent breach of this policy by you may result in disciplinary action being taken against you in accordance with our disciplinary procedure.

12.20 It is a criminal offence to conceal or destroy personal data which is part of a subject access request (see below). This conduct would also amount to gross misconduct under our disciplinary procedure, which could result in your dismissal.

13 How to deal with data breaches

13.1 We have robust measures in place to minimise and prevent data breaches from taking place. Should a breach of personal data occur (whether in respect of you or someone else) then we must take notes and keep evidence of that breach. If the breach is likely to result in a risk to the rights and freedoms of individuals then we must also notify the Information Commissioner's Office within 72 hours.

13.2 If the breach is likely to result in a high risk to the rights and freedoms of individuals, we will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken.

13.3 If you are aware of a data breach you must contact Paul Williamson immediately and keep any evidence you have in relation to the breach.

14 Subject access requests

14.1 All data subjects (employees, customers, suppliers) can make a '**subject access request**' ('SAR') to find out the information we hold about them. This request must be made in writing. If you receive such a request you should forward it immediately to the Data Protection Officer Paul Williamson who will coordinate a response.

14.2 If you would like to make a SAR in relation to your own personal data you should make this in writing to Paul Williamson. We must respond within one month unless the request is complex or numerous in which case the period in which we must respond can be extended by a further two months.

14.3 There is no fee for making a SAR. However, if your request is manifestly unfounded or excessive we may charge a reasonable administrative fee or refuse to respond to your request.

15 Your data subject rights

15.1 You have the right to information about what personal data we process, how and on what basis as set out in this policy.

15.2 You have the right to access your own personal data by way of a subject access request (see above).

15.3 You can correct any inaccuracies in your personal data. To do you should contact Paul Williamson.

15.4 You have the right to request that we erase your personal data where we were not entitled under the law to process it or it is no longer necessary to process it for the purpose it was collected. To do so you should contact Paul Williamson.

15.5 While you are requesting that your personal data is corrected or erased or are contesting the lawfulness of our processing, you can apply for its use to be restricted while the application is made. To do so you should contact Paul Williamson.

15.6 You have the right to object to data processing where we are relying on a legitimate interest to do so and you think that your rights and interests outweigh our own and you wish us to stop.

15.7 You have the right to receive a copy of your personal data and to transfer your personal data to another data controller. We will not charge for this and will in most cases aim to do this within one month.

15.8 With some exceptions, you have the right not to be subjected to automated decision-making.

15.9 You have the right to be notified of a data security breach concerning your personal data.

15.10 In most situations we will not rely on your consent as a lawful ground to process your data. If we do however request your consent to the processing of your personal data for a specific purpose, you have the right not to consent or to withdraw your consent later. To withdraw your consent, you should contact Paul Williamson.

15.11 You have the right to complain to the Information Commissioner. You can do this be contacting the Information Commissioner's Office directly. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk). This website has further information on your rights and our obligations.