

## Data Protection Policy for Employees, Workers and Consultants

### 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 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 and other categories of Data Subjects. A copy of these can be obtained from HR.
- 1.4 The Company has measures in place to protect the security of your data. The organisation has internal policies and controls in place to protect Personal Data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.
- 1.5 The company will hold data in accordance with our **Data Retention Policy**. A copy of this can be obtained from HR. 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 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, or someone else (such as a former employer, your doctor, or a credit reference agency), or it could be created by us. 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.
- 3.4 We will collect and use various types of Personal Data about you, as detailed in our [Privacy Notice](#), a copy of which can be obtained from HR.

### **4. How we define special categories of Personal Data**

- 4.1 **'Special categories of 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; or
- 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 rights in section 12 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.

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.

## **7. Examples of when we might process your Personal Data**

- 7.1 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), as set out in our Privacy Notice, a copy of which can be obtained from HR.

## **8. Sharing your Personal Data**

- 8.1 Sometimes we might share your Personal Data with group companies or our contractors and agents to carry out our obligations under our contract with you or for our legitimate interests.
- 8.2 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.
- 8.3 Legitimate activities which third parties do, are set out in our Privacy Notice, a copy of which can be obtained from HR.
- 8.4 From time to time we may send Personal Data outside the European Economic Area, to CTI in Japan and Waterman in Australia, this is as defined in the Privacy Notice under **"Transferring information outside the EU"**.

## **9. How should you process Personal Data for the Company?**

- 9.1 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 Retention policy**.
- 9.2 The Company's Data Protection Manager, Mark Nuckey, is responsible for reviewing this policy and updating the Board of Directors on the Company's data protection responsibilities and any risks in relation to the processing of data. You should direct any questions in relation to this policy or data protection to this person.
- 9.3 You should only access Personal Data covered by this policy 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.
- 9.4 You should not share Personal Data informally.
  - 9.5 You should keep Personal Data secure and not share it with unauthorised people.
  - 9.6 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.
  - 9.7 You should not make unnecessary copies of Personal Data and should keep and dispose of any copies securely.
  - 9.8 You should use strong passwords.
  - 9.9 You should lock your computer screens when not at your desk.
  - 9.10 Personal Data should be encrypted before being transferred electronically to authorised external contacts. Speak to IT for more information on how to do this.
  - 9.11 Consider anonymising data or using separate keys/codes so that the data subject cannot be identified.
  - 9.12 Do not save Personal Data to your own personal computers or other devices. However, if there is no alternative and there is an explicit operational need to do so, then you must ensure that the device/drive you are using is encrypted.
  - 9.13 Personal Data should never be transferred outside the European Economic Area except in compliance with the law and authorisation of the Data Protection Manager, Mark Nuckey.
  - 9.14 When you are not in your office or at your desk, you must ensure adequate security of personal/sensitive data, so that it is not lying around/visible to others.
  - 9.15 You should not take Personal Data away from Company's premises without authorisation from your line manager or Data Protection Manager.
  - 9.16 Personal Data should be shredded and disposed of securely when you have finished with it.
  - 9.17 You should ask for help from our Data Protection Manager if you are unsure about data protection or if you notice any areas of data protection or security we can improve upon.
  - 9.18 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.
  - 9.19 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.

## 10. How to deal with data breaches

- 10.1 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 within 72 hours we must also notify the Information Commissioner's Office ([www.ico.org.uk](http://www.ico.org.uk)) for UK or, for Ireland, the Data Protection Commission for Ireland ([www.dataprotection.ie](http://www.dataprotection.ie)).
- 10.2 If you are aware of a data breach you must contact Mark Nuckey or [breach@watermangroup.com](mailto:breach@watermangroup.com) immediately and keep any evidence you have in relation to the breach.

## 11. Subject access requests

- 11.1 Data subjects 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 Manager who will coordinate a response.
- 11.2 If you would like to make a SAR in relation to your own Personal Data you should make this in writing to Mark Nuckey. 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.
- 11.3 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.

## 12. Your data subject rights

- 12.1 You have the right to information about what Personal Data we process, how and on what basis as set out in this policy.
- 12.2 You have the right to access your own Personal Data by way of a subject access request (see above).
- 12.3 You can correct any inaccuracies in your Personal Data. To do so you should contact HR.
- 12.4 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 HR.
- 12.5 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 HR.

- 12.6 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.
- 12.7 You have the right to object if we process your Personal Data for the purposes of direct marketing.
- 12.8 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.
- 12.9 With some exceptions, you have the right not to be subjected to automated decision-making.
- 12.10 You have the right to be notified of a data security breach concerning your Personal Data.
- 12.11 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 HR.
- 12.12 You have the right to complain to the Information Commissioner. You can do this by contacting the Information Commissioner's Office directly. Full contact details including a helpline number for the UK can be found on the Information Commissioner's Office website ([www.ico.org.uk](http://www.ico.org.uk)) and, for Ireland, the Data Protection Commission for Ireland ([www.dataprotection.ie](http://www.dataprotection.ie)). These websites have further information on your rights and our obligations.