WENLOCK HEALTH & SAFETY

DATA PROTECTION POLICY

Statement of Intent

This Company is committed to meeting the requirements of the GDPR (General Data Protection Regulation) and current UK data protection legislation in relation to how it collects, processes, records, stores, secures and removes personal data, in manual and electronic form.

Aims

The Company adheres to data protection regulations regarding the collecting, processing, recording, organising, storing, altering, consulting, using, deleting or destroying of personal data from employees, job applicants, sub-contractors and customers. This includes designing, maintaining and reviewing adequate systems, contractual provisions and consent processes to ensure the way it captures, processes, records and stores personal data is safe, secure, robust and appropriate.

The Company will carry out privacy breach risk assessments and use its findings to improve and strengthen its processes and systems. Where appropriate, the Company will provide training to employees and, in particular, those identified as data processors and data controllers.

The Company will carry out comprehensive data protection impact assessments before commissioning or implementing any new projects or systems involving the processing of personal data.

The Company will ensure that no personal data is transferred outside the European Economic Area, unless that country or territory ensures an adequate level of protection.

The Company understands that it will be accountable for the processing, management, regulation, security and retention of all personal data held in manual and electronic form.

Definitions

Personal information means any information relating to an identified or identifiable person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to physical, physiological, mental, economic, cultural or social identity.

Processing Personal Information means any operation which is performed on personal data, whether manually or via automatic means, such as collecting, processing, recording, organising, storing, altering, consulting, using, deleting or destroying.

Data Controller refers to the Company's role in determining the processes to be used when using personal data.

Data Processors refers to the role given to specific employees and specific organisations to process personal data as directed by the Company.

Data Protection Principles

The Company believes its collection, use and storage of personal data is consistent with its employment and business relationships, as well as meeting GDPR's six data protection principles:

1. Personal data must be processed lawfully, fairly and in a transparent manner in relation to an individual
2. Personal data can only be collected for specified, explicit and legitimate purposes
3. Personal data must be adequate, relevant and limited to what is necessary for processing
4. Personal data must be accurate and, where necessary, kept up-to-date

5. Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing
6. Personal data must be processed in a manner that ensures its appropriate security

In addition, personal data will be processed in recognition of an individual's data protection rights ie their right to be informed, right of access, right for inaccuracies to be corrected, right to have information deleted, right to restrict the processing of data, right to portability, right to object to inclusion of any information and right to regulate any automated decision-making and profiling of personal data.

Responsibilities

The Directors have overall and ultimate responsibility for ensuring the Company meets its data protection obligations as a data controller.

All employees are required to comply with data protection legislation, in relation to the use of personal data and treating information confidentially. This includes when handling or processing any personal data in the course of employment relating to employees, job applicants, sub-contractors and customers of the Company, as well as third party data given by customers. Data protection responsibilities will be explained to all new employees at the start of their employment and appropriate information and training will be given where required.

Types of Data Held

The following examples are the main types of personal information that the Company is likely to collect and process. Different types of personal information may be required, depending on particular circumstances, roles, legitimate business interests and legal or contractual requirements. Please note they are for illustrative purposes and are non-exhaustive:

Individual Information: name, address, date of birth

Contact Information/Contact Lists: name, address, telephone, mobile, e-mail addresses

Emergency Contact Information: name, address, telephone, mobile, e-mail addresses of next of kin and relationship to the individual

Suitability to Work: references, interview notes, passport details (or other relevant work permit details), driving licence information, records/results of pre-employment checks, records of qualifications

Information about Skills and Experience: CVs, application forms, references, records of qualifications, skills and training plans, appraisals/performance reviews

Employment Information: Offer letter and contract of employment

Pay Information: bank account details, pay details, tax codes, date of birth, length of service, national insurance or social security numbers, credit/debit receipts for expenses

Benefits Information: length of service, date of birth and health information

Access and security Information: identification codes, entry cards, passwords, security questions, photographs for ID cards

Sickness/Injury Information: sickness self-certification forms, return to work interview forms, fit notes, occupational health information, medical practitioner information, work-related injury or illness information including accident books

Holiday Information: holiday records

Performance Information: records of appraisals/performance reviews, management meeting notes, personal development plans, training plans, personal improvement plans and relevant correspondence

Business Travel Information: driving licence information, vehicle registration, insurance details, Company vehicle tracking information, credit/debit fuel receipts for expenses

Other Employment Information: meeting notes from investigation meetings, disciplinary or grievance meetings, appeal meetings/hearings, relevant recordings and correspondence

Special Category Personal Information

Special Category personal information is sensitive personal data requiring enhanced protection and security, relating to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion and trade union membership. It also includes genetic and biometric data when used for ID purposes. The Company will only use minimal special category personal information, in order to carry out its legal obligations or exercise specific rights under employment law. It therefore does not require individual consent to process special categories of personal information. For example: equal opportunities monitoring, operating sickness absence management procedures or determining reasonable disability adjustments.

The Company will only process health data and medical records from employees for preventative or occupational medicine, assessing work capacity or confirming medical diagnoses to meet legitimate business interests and health and safety legislation. Information will be kept secure at all times and individuals will be kept fully informed regarding its processing and retention.

Reasons for Processing Personal Information

The Company will process personal information for a variety of reasons. The following are examples of key contractual, legitimate and legal reasons. Please note they are for illustrative purposes and are non-exhaustive:

- Personal contact details – for recruitment purposes, carrying out checks in relation to right to work in the UK and the administration and management of employment information
- Contract of employment – for the administration and management of employment
- Payroll, pension and accounts – to calculate and pay remuneration including benefits, pensions and keep accounts relating to the activities of the Company
- Back-up – to ensure the security and accuracy of the data processed by the Company
- Employment administration and management – absence records, holiday, maternity, paternity, adoption and parental leave, equal opportunities, performance management, disciplinary and grievance matters, alleged offences, training and development, health, safety and security, internal communications, information to any government body or agency for legitimate purposes including: social security and income tax

The Company processes the following information about its customers and potential customers for business and marketing requirements:

- Personal contact details – email, address, phone number
- Payment details
- Employee details – name, contact details, qualifications, trade cards/ID
- Details used for RIDDOR reporting and accident investigation
- Details used for health monitoring and medical records
- All of the above for third parties with the purpose of assessing competence levels or accident investigation
- All other data that may be sent to us by a customer without our prior knowledge of the content

The Company will only rarely request employee personal information on the basis of individual consent. Reasons are likely to be limited to organisational marketing and communication purposes, such as through the use of photographs, video or individual profiles for publicity. Individuals will be required to give their

specific consent to be involved and their right to withdraw consent and have any such personal data removed will also be explained.

The Company will also process contract and payment information in regard to its sub-contractors to meet its contractual, legal and legitimate business interests. It will also process and store evidence of relevant skills and qualifications to meet its contractual, legal and legitimate business interests, including assessment of suitability for the work that is carried out on the Company's behalf.

Data Disclosures

Employee personal data will be shared with some colleagues within the Company where it is necessary for them to carry out their data processing duties.

The Company may make personal data relating to employees available to those who provide relevant external products or services to the Company such as sub-contracted professional business advisers, payroll and/or pension administrators, regulatory authorities and governmental organisations, based on lawful or contractual necessity, or for legitimate business interests, covering areas including, but not limited to:

- administration and management of personnel data
- employee pay, statutory payments, remuneration and benefits
- employee insurance policies, benefits or pension plans
- CVs, application forms, references and other information gathered by external recruiters
- assessing reasonable adjustments for disabled employees
- assistance with grievance or disciplinary issues
- management training and development
- business coaching and mentoring
- compliance with health and safety or occupational health obligations towards an employee
- HR/legal advice and guidance

These types of disclosures will only be made when strictly necessary and for defined purposes.

The Company will make personal data belonging to customers available to colleagues within the Company when necessary and relevant. Customers' personal details will be passed to a third party only when specifically requested by the customer. This may include a requirement for additional services provided by a third party, such as HR or training. Further details of this can be found in the Company Terms and Conditions sent to all customers, for which consent will be requested and obtained prior to the service being undertaken.

Security of Personal Information

The Company routinely checks its organisational and technical security measures to guard against the unauthorised access, improper use, alteration, destruction or accidental loss of personal information.

Personal data must not be shared informally, disclosed to unauthorised people either within or outside the Company, or deleted in error either through negligence, carelessness or recklessness. Personal data must be kept secure at all times.

The Company protects all servers and computers containing electronic personal data through the use of approved security software and firewalls and carries out a sequence of regular back-ups and system updates. When data is stored electronically, it must be protected from unauthorised access using strong passwords which are changed regularly and never shared between employees.

Personal data should only be stored on designated drives and servers and must only be uploaded to Company approved cloud computing services. When working with personal data, employees must ensure data is entered accurately and computer screens are always locked when left unattended. Personal data should never be kept or transported on laptops, USB sticks or other mobile devices such as tablets or smart phones, unless authorised by a Director. Paper copies and data printouts containing personal data must be stored in dedicated lockable storage units.

Employees handling personal data also have a responsibility for making sure data held is kept up-to-date and stored in as few places as necessary.

Data printouts containing personal information should be shredded and disposed of securely when storage time limits have elapsed. Electronic files containing personal information should be safely deleted from Company servers, computers and cloud storage, when storage time limits have elapsed.

Employees are also required to familiarise themselves with the Company's IT Communications, Security and Confidentiality instructions. If employees are unsure of their obligations, they must seek clarification from a Director. If any employees fail to comply with these obligations, their failure will be regarded as serious misconduct and will result in disciplinary action.

If personal information requires processing by a sub-contractor, such as an external professional adviser, the sub-contractor will be asked to demonstrate their compliance with the Company's security requirements, to ensure the careful handling and protection of personal information outside the Company. All subcontracted processors take instruction from the Company and their obligations with regard to what information they process and what they can do with it are contractually agreed.

If the Company needs to disclose personal information to HMRC and/or other authorities to meet legitimate and legal obligations, it will ensure only relevant and accurate information is sent using secure channels.

Data Protection Risk Assessments

The Company carries out periodic privacy breach risk assessments on the personal data that it collects, processes, records, stores, secures and deletes to meet its data protection obligations and also strengthen its processes and systems. The Company has put in place procedures to detect, report and investigate any suspected or actual personal data breaches ie a breach of security that leads to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. It is aware of its duty to report significant breaches that cause significant harm to the affected individuals to the Information Commissioner and is aware of the possible consequences.

Automated Decision Making

No decision will be made about employees solely on the basis of automated decision making (ie where a recruitment decision is taken about an employee using an electronic system without human involvement).

Safe Deletion or Destruction of Personal Information

The Company ensures that personal information is only kept for reasonable periods of time to meet its legitimate employment, contractual and legal obligations.

Personnel information will be reviewed when employees leave the organisation and some data eg emergency contact information, will be destroyed, via in situ shredding or electronic data deletion.

Where documents may be relevant to a contractual claim linked to employment eg contracts of employment and contact details, they will be securely stored for a maximum of seven years following termination of employment (to meet the UK Limitations Act 1980 regarding the time limits for bringing a claim and additional reasonable time to deal with any relevant investigation), then safely destroyed via in situ shredding. Relevant electronic data will also be securely stored for up to seven years following termination of employment, then deleted from Company devices, hardware and cloud storage.

The Company will only provide standard written references up to a maximum of seven years following termination of employment.

Other specific documentation retention periods may also be applicable to your personal data:

Application forms and interview notes for unsuccessful candidates: up to one year to meet relevant retention periods regarding discrimination under the Equality Act 2010 and extension periods.

National Minimum Wage records: up to three years after the end of the pay reference period following the one that the records cover to meet the National Minimum Wage Act 1998.

Records relating to Working Time: up to two years from the date on which they were made to meet Working Time Regulations 1998 (SI 1998/1833).

Wage/Salary Records: up to six years to meet Taxes Management Act 1970

Statutory Maternity records, calculations, certificates or other medical evidence: up to three years after the end of the tax year in which the maternity period ends to meet the Statutory Maternity Pay (General) Regulations 1986 (SI 1995/3136) as amended and Limitations Act 1980.

For legitimate reasons relating to other Health and Safety Legislation, the Company will keep certain personal data for up to forty years (e.g. where there has been a breach of the Control of Asbestos Regulations 2012).

Most personal data will be held for the required time over and above the duration of your agreement with the Company.

Privacy Notices

In addition to this Policy, the Company provides further information to employees, job applicants, sub-contractors and customers in the form of 'Privacy Notices' regarding how and why it is collecting, processing, recording, organising, storing, altering, consulting, using, or deleting personal data, along with relevant security information and details regarding the giving of their consent, the right of access to their personal information and the right to have their information deleted, where applicable.

Accessing Personal Information

Individuals have a legal right to make a request to the Company for disclosure of copies of personal information on them which is being processed by the Company: this is called a *Subject Access Request*. The Company seeks to process any such requests as quickly as possible, but within one month of the date of receipt. In some cases, the data will be exempt from the disclosure requirement, but if this applies, the individual will be informed. The Company will seek additional information from the individual to deal with the request along with proof of identity.

Data Protection Impact Assessments

The Company ensures that privacy and data protection are key considerations during the early stages of any new project and then throughout its lifecycle, including new IT systems for storing and accessing personal data; developing policies or strategies that have privacy implications; and any initiatives that may involve data sharing or using data for new purposes.

Issue Date: 23 May 2018