Data Protection Policy

The Data Protection Acts 1988 and 2003 apply to the processing of personal data. This company is committed to complying with its legal obligations in this regard. The company collects and processes personal data relating to its team members in the course of business in a variety of circumstances, e.g., recruitment, training, payment, performance reviews, and to protect the legitimate interests of the company.

This policy covers any individual about whom this company processes data. This may include current and former team members. Processing of data includes: collecting; recording; storing; altering; disclosing; destroying; and blocking.

Personal data kept by this company shall normally be stored on the team member's personnel file or Human Resources electronic database. Highly sensitive data, such as medical information, will be stored in a separate file, in order to ensure the highest levels of confidentiality. The company will ensure that only authorised personnel have access to a team member's personnel file.

It may be necessary to store certain other personal data outside Human Resources, e.g., salary details will be stored in the payroll department. The team member's Manager or supervisor may have access to certain personal data where necessary. The company has appropriate security measures in place to protect against unauthorised access.

Collection and storage of data

This company processes certain data relevant to the nature of the employment regarding its team members and, where necessary, to protect its legitimate business interests. We will ensure that personal data will be processed in accordance with the principles of data protection, as described in the Data Protection Acts 1988 and 2003.

Personal data is normally obtained directly from the team member concerned. In certain circumstances, it will, however, be necessary to obtain data from third parties, e.g., references

from previous employers. Where relevant to the nature of the work, the company may make an application to the Garda Vetting Bureau for Garda clearance of a team member.

Personal data collected by the company is used for ordinary personnel management purposes. Where there is a need to collect data for another purpose, the company shall inform you of this. In cases where it is appropriate to get your consent to such processing, the company will do so.

Team members are responsible for ensuring that they inform Human Resources of any changes in their personal details, e.g., change of address. Managers and supervisors must inform Human Resources of any changes in team members' personal details, e.g., promotion, pay increases. We endeavour to ensure personal data held by the company is up to date and accurate.

The company is under legal obligation to keep certain data for a specified period of time. In addition, the company will need to keep personnel data for a period of time in order to protect its legitimate interests.

Security and Disclosure of Data

The company will take all reasonable steps to ensure that appropriate security measures are in place to protect the confidentiality of both electronic and manual data. Security measures will be reviewed from time to time, having regard to the technology available, the cost and the risk of unauthorised access. Team members must implement all company security policies and procedures, e.g., use of computer passwords, locking filing cabinets.

Human Resources data will only be processed for employment-related purposes and, in general, will not be disclosed to third parties, except where required or authorised by law or with the agreement of the team member. Human Resources files are electronically stored and team members who have access to these files must ensure that they treat them confidentially. Team members working in the payroll department must treat all personal data they receive confidentially and must not disclose it, except in the course of their employment. Broadline Group Human Resources Manager may request this information.

All team members will have access to a certain amount of personal data relating to colleagues, clients, candidates and other third parties. Team members must play their part in ensuring its confidentiality. They must adhere to the data protection principles and must not disclose such

data, except where necessary in the course of their employment, or in accordance with law. They must not remove or destroy personal data except for lawful reasons.

Any breach of the data protection principles is a serious matter and may lead to disciplinary action up to and including dismissal. If team members are in any doubt regarding their obligations, they should contact the Human Resources Manager.

Medical Data

The company carries out pre-employment medical questionnaires as part of the recruitment process. This data will be retained by the company. Occasionally, it may be necessary to refer team members to the company's doctor for a medical opinion and all team members are required by their contract of employment to attend in this case. The company may receive certain medical information, which will be stored in a secure manner with the utmost regard for the confidentiality of the document. The company does not retain medical reports on job applicants who do not become team members for longer than is necessary.

Team members are entitled to request access to their medical reports. Should a team member wish to do so, please contact Human Resources, which will consult with the doctor who examined you and request the data. The final decision lies with the doctor. Team members are required to submit sick certificates in accordance with the company policy. These will be stored by the company, having the utmost regard for their confidentiality.

Closed Circuit Monitoring

The company has closed circuit television cameras located throughout the building and grounds. This is necessary in order to protect against theft or pilferage, for the security of team members and company property. Access to the recorded material will be strictly limited to authorised personnel. Closed circuit surveillance is used to manage performance and may be used in the course of an investigation under the company's disciplinary procedures or bullying and harassment procedures.

Data Protection Officer

The Managing Director is the data protection officer for this company. They bear overall responsibility for ensuring compliance with data protection legislation. All team members must co-operate with the data protection officer when carrying out their duties.

The data protection officer is also available to answer queries or deal with team members' concerns about data protection.

Access Requests

Team members are entitled to request data held about them on computer or in relevant filing sets. The company will provide this data within 40 days. There is a charge of €6.35 for requesting this data.

A team member should make a request in writing to the data protection officer, stating the exact data required. Team members are only entitled to access data about themselves and will not be provided with data relating to other team members or third parties. It may be possible to block out data relating to a third party or conceal their identity, and if this is possible the company may do so.

Data that is classified as the opinion of another person will be provided unless it was given on the understanding that it will be treated confidentially. Team members who express opinions about other team members in the course of their employment should bear in mind that their opinion may be disclosed in an access request, e.g., performance appraisals.

A team member who is dissatisfied with the outcome of an access request has the option of using the company's grievance procedure.

Right to Object

Team members have the right to object to data processing that is causing them distress. Where such objection is justified, the company will cease processing the data unless it has a legitimate interest that prevents this. The company will make every effort to alleviate the distress caused to the individual.

An objection should be made in writing to the data protection officer, outlining the data in question and the harm being caused to the team member.

Confidentiality

Every effort it taken by the company to ensure that clients' affairs are treated with absolute confidentiality. You will be expected to keep all information concerning the company, its stakeholders, third parties, and any other connected company with whom are involved as an team member of this company, absolutely confidential. Any deliberate breach of confidence will be regarded as a matter justifying summary dismissal. This requirement for confidentiality extends beyond your period of employment.

You will deliver to the company, on termination of your employment, or at any time it may so request, all documents, notes, records, manuals and any other materials or property belonging to the company which you may then possess or have under your control. You may not, with company consent, keep copies of same.

You may not remove from the company's premises at any time, without proper advance written authorisation, any document or other property which belongs to the company or contains or refers to any confidential information relating to the company, its clients, candidates, team members or third parties. You will return to the company, prior to termination of your employment, any documents or other company property that subsequently comes into your procession or procurement in the future.

You are not permitted to make any press, radio or TV statements nor to publish or submit for publication any letters, or articles about the business or affairs of the company or management company. You must not divulge to any other sources any sensitive, compromising or financial information without the written permission of the Managing Director. This will apply even after you are no longer a team member.

You will be expected to devote your entire working time and attention to the company's affairs and therefore you may not, without the prior written consent of the company, be involved, in any outside business or enterprise.

Sales Data Bases / Financial information

You must not pass on any information to any third-party regarding stakeholder's home addresses phone number, email address, credit card details etc to any third parties. You must not pass on any information to any past team member who had request such information. Any breaches of this policy may lead to disciplinary action, up to and including dismissal.