POLICY STATEMENT POL12
DATA PROTECTION

General Policy Statements

All companies using and storing confidential and personal data are required by law to be registered under the Data Protection Act, 2018, (DPA).

It is the company's policy to ensure that personal data held by the company about its employees, customers, suppliers and all other individuals is processed fairly and lawfully. The company will take all necessary steps to implement this policy and ensure that the company's internal procedures are monitored periodically to ensure compliance.

The following notes summarise the lengthy and complex legislation that governs the storage and disclosure of personal data.

It is a criminal offence, not a civil offence, for the company or an individual knowingly or recklessly to:

- Hold or use personal data for a non-registered purpose
- Obtain personal data for a non-registered purpose
- Disclose personal data to a non-registered source

Anyone who falls foul of the DPA will risk having a criminal police record.

Policy Objectives

We will strive to meet all eight of the Data Protection Principles:

1. Personal data shall be processed fairly and lawfully.
2. Personal data shall be obtained only for one or more specified and lawful purpose and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under the Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Responsibility

Data protection is a responsibility shared by all employees and agents of the company. Employees are

expected to be familiar with, and observe at all times, the policy and procedures relating to data protection and any additional instructions which may be issued from time to time.

The person having overall responsibility for data protection within the company will be the Data Protection Compliance Officer.

Each manager and supervisor will have responsibility for data protection matters in his/her own immediate area of work.

PROCESSING DATA - DEBTORS

The company is entitled to collect and hold information concerning individuals it is pursuing under a court warrant / order. It is further entitled to pass this information between itself and its clients; so much as it concerns the execution and reporting of warrants.

The following procedure will ensure compliance when dealing with incoming telephone calls:

1. Ask for the case reference number; either ours or the clients
2. Ask for the name of the caller and confirm it is the debtor using relevant security questions, or
3. Ask for and record the client caller's name

You must not give personal data (details of the debtor's account/ offence/ address/ contact number) to a friend, relation or organisation (e.g. Citizens Advice), unless [written] authority has been provided by the debtor. If you cannot confirm the identity of the caller as that of the debtor or client, you must advise him/her politely that under the requirements of DPA you cannot furnish any specific details. If the caller is persistent, advise your manager.

There are certain occasions when the duty of confidentiality under the DPA is superseded. These occasions are fairly exceptional and most will never need concern employees and are therefore not listed here.

As noted, breaches of the DPA can result in criminal prosecutions. If staff are found to be knowingly in breach of the DPA, regardless of whether the Information Commissioner (the controller of the DPA) takes action, disciplinary action for misconduct will certainly result (including the possibility of summary dismissal).

PROCESSING DATA - EMPLOYEES

General

The company will hold personal data about its employees in its manual and automated filing systems. Personal data may be processed for the purposes of:

- salary administration
- pension administration
- health administration
- health insurance/benefits
- training and appraisal including performance records
- disciplinary and grievance records
- company car fleet/leasing administration

- any company benefit administration
- where the nature of an employee's employment makes it necessary or desirable for the benefit of the company, personal information relating to that employee may be disclosed for marketing and/or PR purposes and in connection with the performance of that employee's duties.
- any potential sale of over 50% of the shares of the company or other changes of control or any potential transfer of an employee's employment under the Transfer of Undertakings (Protection of Employment) Regulations 1981. Disclosure may include, in the case of sale, change of control or transfer, disclosure to the potential purchaser or investor and their advisors.

In certain circumstances the company is required to obtain the employee's consent to process personal data. From time to time, the company will also need to process sensitive personal data about its employees.

Such data is broadly defined as including details of an individual's ethnic or racial origins, political opinions, religious or other beliefs, trade union membership, physical or mental health, or data relating to the commission (or alleged commission) of any criminal offence or convictions. The employee's explicit consent will be obtained before processing this data.

The consent of employees for the processing of data will have been obtained by the company as part of its basic contract of employment. Employees will be informed where data needs to be processed for additional purposes, and the company will state:

- the purpose or purposes for which the data is intended to be processed; and
- the identity of the company's nominated representative (Data Protection Compliance Officer);

Rights of Employees

The Act allows employees to find out what information is held about themselves on computer and in some paper records. Employees wishing to obtain a copy of personal data held by the company must make a written request to the Data Protection Officer who will deal with the request in accordance with the Act.

SECURITY OF DATA

Employees who are required as part of their job description to process personal data about employees or customers, will receive training and guidance on the security of data to ensure that all data is processed fairly and lawfully. However, we expect all employees to be aware of the basic principles as set out in this policy. In particular employees should be aware of the following:

- All personal data held by the company must be treated as strictly confidential.
- Personal data must not be disclosed to anyone outside the company unless the individual concerned has consented to such disclosure, or the Data Protection Compliance Officer has given a specific instruction to do so.
- Personal data must be kept secure at all times. Personal data must not be left unattended unless it has been placed in a secure location. Relevant employees will be advised by the Data Protection Compliance Officer of the physical security of arrangements to be adopted appropriate to the level of confidentiality of the personal data concerned.
- Personal data must not be copied (whether on computer, media, photocopies, computer print outs,

or otherwise) without documented authorisation from management.

- Personal data must not be removed or transferred from the company's premises (whether on computer media, in hard copy form, or otherwise) without documented authorisation from management.
- It is the responsibility of all employees to report all security breaches, or suspected security breaches, relating to unauthorised access to, or disclosure of personal data, to the Data Protection Compliance Officer.
- Drivers must not leave sensitive information in a vehicle over night or for any extended period during the day. This includes warrants, copy warrants, reports, receipt books, identity cards and associated documentation.

Breaches of these guidelines may lead to disciplinary action and depending on the seriousness of the breach, may lead to summary dismissal. Breaches of these guidelines may also constitute a criminal offence.

REVIEW

Execution of this policy is the responsibility of the directors.

This policy will be reviewed during management review meetings and more often if there are significant changes.

[redacted]

[redacted] Managing Director

18 December 2024