



DATA PROTECTION POLICY

Introduction

Trustseal recognises and accepts its responsibility as set out in the General Data Protection Regulation 2018 and the sub-legislation contained therein. The Finance Director (Joint Managing Director) as a data controller, will take all reasonable steps to meet this responsibility and to promote good practice in the handling and use of personal information. To comply with the data protection principles set out in the 2018 Regulation. This policy statement applies to all suppliers, customers, contractors and employees, and individuals about whom the company processes personal information, as well as other partners and companies with which Trustseal undertakes its business.

Scope

The company needs to collect and use certain types of personal information about people with whom it deals to operate. These include current, past, and prospective employees, suppliers, customers, contractors, and others with whom it communicates. In addition, it may be required by law to collect and use certain types of information to comply with the requirements of government departments. This personal information will be dealt with properly however it is collected, recorded, and used – whether on paper, in a computer, or recorded on other material – and there are safeguards to ensure this in the General Data Protection Regulation 2018. We regard the lawful and correct treatment of personal information as essential to secure the successful carrying out of operations and the delivery of our services, and for maintaining confidence with those whom we deal. The company wishes to ensure that it treats personal information lawfully, correctly and in compliance with the 2018 Regulation. To this end we fully endorse the obligations of the Regulation and adhere to the principles of data protection.

The following paragraphs provide a brief aid to the General Data Protection Regulation 2018.

1. Main provisions of the General Data Protection Regulation 2018

- a) Ensuring data controllers notify their processing of personal data with the Information Commissioners Office. The company will supply certain information to the Commissioner who maintains a public register of the types of information organisations process, where it gets it from and what it does with it.
- b) Observing the eight Data Protection Principles shown below.
- c) Allowing the data subject to exercise his/her rights and have right of access to their personal Information; what is held, how it is processed, to whom it is disclosed and to be told of the logic behind automated decisions. Such access requests must be complied with within 40 days and the maximum chargeable fee is £10.

2. Definitions

Data Controller Any individual or organisation who controls personal data, in this instance, the Joint Managing Director.

Personal Data: Information held on a relevant filing system, accessible record or computerised record (as well as digital audio or video equipment), which identifies living individuals.

Sensitive Personal Data: Personal data relating to an individual's race or ethnic origin, political opinions, religious or philosophical beliefs, physical/mental health, trade union membership, sexual orientation, personal life and criminal activities.

Relevant Filing System: Also known as manual records i.e. a set of records which are organised by reference to the individual/their criteria and are structured in such a way as to make specific information readily accessible e.g. customer or supplier records, microfilm readers and records.

Data Subject: An individual who is the subject of the personal data, for example, employees, contractors, customers, job applicants etc.

Processing: Obtaining, recording, or holding data or carrying out any operation on the data including organising, adapting, altering, retrieving, consulting, using, disclosing, disseminating, aligning, blocking, erasing or destroying the data.

Accessible Records Any records which are kept by the company as part of a statutory duty, e.g. payroll records, company accounts records.

3. Data Protection Principles

Specifically, the principles require that personal information:

1. shall be processed fairly and lawfully and shall not be processed unless specific conditions as set out in the 1998 Act are met.
2. shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. shall be adequate, relevant, and not excessive in relation to the purpose or purposes for which they are processed.
4. shall be accurate and, where necessary, kept up to date.
5. shall not be kept for longer than is necessary for that purpose or those purposes.
6. shall be processed in accordance with the rights of the data subject under the 1998 Act.
7. appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. shall not be transferred to a country or territory outside the European Union 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.

Commitment

The company and Joint Managing Directors will, through appropriate management and application of criteria and controls:

- Observe fully the conditions regarding the fair collection and use of information.
- Meet its legal obligations to specify the purposes for which information is used.
- Collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements.
- Ensure the quality of the information used, including its accuracy and relevancy for the purpose(s) specified.
- Apply strict checks to determine the length of time information is held.
- Ensure that the rights of people about whom information is held can be fully exercised under the 1998 Act. (These include: the right to be informed that processing is being undertaken; the right of access to one's personal information; the right to prevent processing in certain circumstances; the right to correct, block or erase information which is regarded as erroneous)
- Take appropriate technical and organisational security measures to safeguard personal information.
- Ensure that personal information is not transferred abroad without suitable safeguards.

Compliance

In addition, the Data Controller will take steps to ensure that:

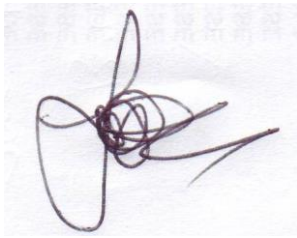
- There is someone with specific responsibility for data protection in the organisation.
- Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice.
- Everyone managing and handling personal information is appropriately trained to do so.
- Everyone managing and handling personal information is appropriately supervised.
- Anybody wanting to make enquiries about handling personal information knows what to do.
- Queries about handling personal information are promptly and courteously dealt with.
- Methods of handling personal information are clearly described.
- A regular review and audit are made of the way personal information is managed.
- Methods of handling personal information are regularly assessed and evaluated.
- Performance of handling personal information is regularly assessed and evaluated.
- It disseminates to employees information on good practice in respect of handling, using, and storing personal information.

Data Protection and Access – Employment

The company holds personnel records for each employee containing information such as an application form or employee sheet together with standard employment documents including training, appraisals, disciplinary/grievance matters, attendance and timekeeping, medical records, health and safety, and general correspondence. This information is only processed for personnel administration, payroll, statutory compliance, and employment purposes.

These principles, procedures, and practice also apply to data concerning job applicants and former employees.

The company also holds pay and tax data in accordance with statutory requirements. The company complies with the above Data Protection principles and will not disclose information about employees without permission unless required to do so by authorised statutory bodies. All queries about employment data should be referred to a director or senior executive.

A handwritten signature in dark ink, appearing to be 'Jon Wragg', written on a light-colored background.

Jon Wragg

Date 16/03/23

Managing Directors