manyother ltd

Data Protection Policy

(V2.0 – last updated Feb. 2020)

1. Introduction

This Policy forms part of a suite of policies and procedures that support an information governance framework.

The Company needs to hold and to process large amounts of personal data about its customers, employees, contractors and other individuals in order to carry out its business and organisational functions. Data protection law defines personal data as any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. This information is often referred to as person identifying information (PII) by the Company and for the purposes of this Policy should be considered to have the same meaning as personal data as defined by legislation.

2. Purpose

Compliance with legislation will be achieved through the implementation of controls and responsibilities including measures to ensure that:

- 2.1 personal data is processed lawfully, fairly and transparently. This includes the provision of appropriate information to individuals upon collection of their data by the Company in the form of our Consent to use Personal Data policy.
- 2.2 personal data is processed only for the purposes for which it was collected.
- 2.3 personal data is adequate, relevant and not excessive for the purposes for which it was collected.
- 2.4 personal data is accurate and where necessary kept up to date.
- 2.5 personal data is not kept for longer than necessary.
- 2.6 personal data is processed in accordance with integrity and confidentiality principles; this includes physical and organisational measures to ensure that personal data, both manual and digital, are subject to an appropriate level of security when stored, used and communicated by the Company, in order to protect against unlawful or malicious processing and accidental loss, destruction or damage. It also includes measures to ensure that personal data transferred to or otherwise shared with third parties have appropriate contractual provisions applied.
- 2.7 personal data is processed in accordance with the rights of individuals, where applicable. These rights are:
    - the right to be informed.
    - the right of access to the information held about them by the Company (through a subject access request)

- the right to rectification.
- the right to erase the data subject.
- the right to restrict processing.
- the right to data portability to the data subject.
- the right to object.

- 2.8 The design and implementation of Company systems and processes make provision for the security and privacy of personal data.
- 2.9 Personal data will not be transferred outside of the European Economic Area (EEA) without appropriate safeguards in place
- 2.10 Additional conditions and safeguards must be applied to ensure that more sensitive personal data (defined as Special Category data in the legislation), is handled appropriately by the Company. Special category personal data is personal data relating to an individual's:
  - race or ethnic origin.
  - political opinions.
  - religious or philosophical beliefs.
  - trade union membership.
  - genetic data.
  - health or sex life or sexual orientation.

In addition, similar extra conditions and safeguards also apply to the processing of the personal data relating to criminal convictions and offences.

3. Scope

This Policy applies to:

- all personal data held and processed by the Company. This includes expressions of opinion about the individual and of the intentions of the Company in respect of that individual. It includes data held in any system or format, whether electronic or manual.
- all members of staff, as well as individuals conducting work at or for the Company and/or its subsidiaries, who have access to Company information. This includes temporary, visiting, casual, voluntary and agency workers and suppliers. (this list is not intended to be exhaustive).
- all locations from which personal data is accessed.

4. Responsibilities and compliance framework

All staff and other approved users of Company systems must:

- complete data protection training every two years and must seek advice and guidance from the Company if clarification is required.

- immediately report any actual or suspected misuse, unauthorised disclosure or exposure of personal data, “near misses” or working practices which jeopardise the security of personal data held by the Company.

Directors and Managers are responsible for ensuring that personal data within their areas is processed in line with this Policy and established procedures.

Staff or subcontractors must note that any breach of this Policy may be treated as misconduct under the Companies relevant disciplinary procedures and could lead to disciplinary action or sanctions. Serious breaches of this Policy may constitute gross misconduct and lead to summary dismissal or termination of contract.

5. Monitoring compliance

This Policy and its implementation are subject to internal monitoring and auditing throughout the Company and the outcomes from these processes will inform and improve practices as part of a commitment to continual improvement. The Company will also undertake appropriate benchmarking and may be audited by external bodies as required.

Reports on matters related to this Policy will be provided to the Directors.

6. Review of Policy

This Policy will be reviewed at least annually or when significant changes are required.

End of Document