OT Group ("the Company") GDPR Data Protection Policy

1. Introduction

The Company is committed to a policy of protecting the rights and privacy of individuals in accordance with the General Data Protection Regulation ("the Regulation"). The Company collects and uses information about people with whom it communicates. This policy describes how this Personal Data must be collected, handled and stored to meet the Company's data protection standards – and to comply with the law.

2. Scope

This policy applies to the Company where a Data Subject's Personal Data is processed in the context of the business activities of the Company. This policy applies to all Processing of Personal Data in electronic form (including e-mail and documents) or where it is held in manual files that contain information about individuals.

3. Definitions

Data Controller	Person or body who determines the purposes for which, and the manner in which, any Personal Data is processed.
Data Protection	The process of safeguarding Personal Data from unauthorised or unlawful disclosure, access, alteration, Processing, transfer or destruction.
Data Subject	An individual about whom Personal Data is held.
Personal Data	Any information which enables a Data Subject to be identified.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.
Processing, Process or Processed	Obtaining, recording, holding or carrying out any operation or set of operations on Personal Data including organising, amending, retrieving, using, disclosing, erasing or destroying such Personal Data.
Third Party	Another entity who is authorised by the Company to Process Personal Data relating to the Company's Data Subjects.

4. Policy

4.1 Responsibility

The Board of Directors is ultimately responsible for ensuring that the Company meets its legal obligations. The Company have appointed a Data Security Manager who reports to the Board.

The Duties of the Data Security Manager include:

- Ensuring compliance with this Policy and reviewing and updating the Policy from time to time.
- Reviewing all Data Protection procedures and related policies.
- Keeping the Board updated about data protection responsibilities, risk and issues.
- Acting as a point of contact.
- Checking and approving any contracts or agreements with Third Parties that may handle Personal Data.
- Ensuring that everyone processing Personal Data understands that they are contractually responsible for following good data protection practice and are appropriately trained to do so.

The Board will ensure that all employees responsible for Processing of Personal Data are aware of and comply with the contents of this Policy.

4.2 Data Protection Principles

The Company has adopted the eight Data Protection principles in the Regulation:

(a) Personal Data shall be processed **lawfully and fairly**. Data Subjects will be advised of the Processing of their Personal Data and it must be for one of the purposes specified in the applicable Data Protection regulation.

(b) Personal Data shall be collected and **Processed only for specific and lawful purposes**. The Company will specify what the Personal Data will be used for and Process that Personal Data only to meet the specified purpose.

(c) Personal Data shall be **adequate, relevant and not excessive** in relation to the purpose for which it is Processed. The Company will not store any Personal Data that is not required.

(d) Personal Data shall be **accurate and where necessary kept up to date**. Data Subjects should ensure that they provide accurate and up to date information. The Company will adopt all necessary measures to ensure that the Personal Data it collects and Processes is complete and accurate, and updated as necessary.

(e) Personal Data shall be **kept for as long as is necessary** for the purposes for which the Personal Data is Processed. The Company shall retain Personal Data in compliance with the Regulation and any statutory requirements. Personal Data will be disposed of securely.

Personal Data shall be Processed in accordance with the **rights of the Data Subject**. The Company shall ensure that Data Subject rights are maintained and shall only Process Personal Data in accordance with those rights.

Data Subjects have a right to:

- request access to any data held about them by a Data Controller;
- prevent the Processing of their Personal Data for direct-marketing purposes;
- ask to have inaccurate Personal Data amended; and
- prevent Processing that is likely to cause damage or distress to themselves or anyone else.

(f) The Company shall put in place **relevant technical and organisation measures** to ensure the integrity and confidentiality of Personal Data is maintained at all times. This includes the prevention of loss or damage, unauthorised access or Processing, and other risks to which it might be exposed.

(g) The Company shall ensure that **Personal Data is not transferred to a country or a territory outside the EEA** unless that country or territory has an adequate level of protection for the rights and freedoms of Data Subjects.

4.3 Data Processing

The Regulation is intended not to prevent the processing of Personal Data, but to ensure that it is done fairly and without adversely affecting the rights of the Data Subject.

Special Categories of Data (also known as sensitive data) will only be processed when necessary to defend legal or insurance claims or specifically authorised by law.

For Personal Data to be processed lawfully, certain specific conditions have to be met. These include, among other things, requirements that the Data Subject has consented to the Processing, or that the Processing is necessary for the legitimate interest of the Data Controller or the party to whom the Personal Data is disclosed.

4.4 Marketing

The Company will send selected marketing on a business to business basis to existing and potential customers, but always provide the ability to opt out via a preference centre.

4. 5 Data Subject Requests

The Company will establish a system to enable all Data Subjects to exercise their rights to:

- Access to Information
- Object or restrict Processing Data portability, rectification or erasure

All requests will be considered in accordance with the Regulation.

All Data Subjects are entitled, subject to verification of their identity, to request:

- the purposes of the collection, Processing, use and storage of their Personal Data;
- the source(s) of the Personal Data, if not obtained from the Data Subject;
- the categories of Personal Data stored for the Data Subject;
- the recipients or categories of recipients to whom the Personal Data has been or may be transmitted, as well as their location;
- the retention period or rationale for determining the retention period.

All requests should be made to gdpr@officeteam.co.uk.

As a result of the request, if the Data Subject wishes to object the Processing of their Personal Data, request rectification or erasure, or have any queries, these should also be made to gdpr@officeteam.co.uk.

A response to either a request for their Personal Data or any other matter will be provided within 30 days of the request, once identity has been confirmed.

In certain circumstances the Company may be required to disclose data which does not require the consent of the Data Subject, such as to law enforcement agencies. The Company will ensure the request is legitimate, seeking assistance from the Board or Company's legal advisers where necessary.

4.5 Data Protection Training

All staff who handle Personal Data will have their responsibilities under this policy explained to them. In addition Data Protection training and procedural guidance will be provided to staff.

4.6 Breach or Complaint Reporting

Any individual who believes that a Personal Data Breach has taken place must immediately notify the Data Security Manager (gdpr@officeteam.co.uk). An investigation will be carried out and the individual will be kept informed. The Company will adopt its Breach Reporting procedure and determine whether a Personal Data Breach has occurred and report to the relevant authority where appropriate.

4.7 Review of Policy

This policy shall be reviewed on an annual basis, or more frequently if legislation changes.