General Data Protection Policy

1. Introduction

This Policy sets out the obligations of the Modular 500 Limited ("the Company") regarding data protection and the rights of individuals ("data subjects") in respect of their personal data under the General Data Protection Regulation ("the Regulation").

The Regulation defines "personal data" as any information relating to an identified or identifiable living person (a 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 Policy sets out the procedures that are to be followed when dealing with personal data. The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company. The Company is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

Contact information for the Company's data protection officer is:

Matthew Taylor

E-mail: mt@modular500.com

Phone: +44 (0) 1246 914 005

Mobile: +44(0) 7525338707

2. The Data Protection Principles

All personal data must be:

a) processed lawfully, fairly, and in a transparent manner in relation to the data subject;

e.g. You need to be clear why you are collecting data and what it will be used for.

b) collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3. Lawful, Fair, and Transparent Data Processing

The Regulation states that processing of personal data shall be lawful if at least one of the following applies:

a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes.

b) processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract.

c) processing is necessary for compliance with a legal obligation to which the controller is subject.

d) processing is necessary to protect the interests of the data subject or of another person.

e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

f) processing is necessary for the purposes of the legitimate interest pursued by the controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

4. Processed for Specified, Explicit and Legitimate Purposes

4.1 The Company collects and processes the personal data set out in Part 21 of this Policy. This may include personal data received directly from data subjects (for example, contact details used when a data subject communicates, contracts or transacts business with us) and data received from third parties (e.g. statutory bodies etc).

4.2 The Company only processes personal data for the specific purposes set out in Part 21 of this Policy (or for other purposes expressly permitted by the Regulation).

5. Adequate, Relevant and Limited Data Processing

The Company will only collect and process personal data for and to the extent necessary for the specific purpose(s) informed to data subjects as under Part 4, above.

6. Accuracy of Data and Keeping Data Up To Date

The Company shall ensure that all personal data collected and processed is kept accurate and up-to-date. The accuracy of data shall be checked when it is collected and at regular intervals thereafter. Where any inaccurate or out-of-date data is found, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

7. Timely Processing

The Company shall not keep personal data for any longer than is necessary in light of the purposes for which that data was originally collected and processed.

8. Secure Processing

The Company shall ensure that all personal data collected and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. Further details of the data protection and organisational measures which shall be taken are provided in Parts 22 and 23 of this Policy.

9. Accountability

9.1 The Company's data protection officer is **Matthew Taylor**.

9.2 The Company's Data Protection officer shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

a) The purposes for which the company processes personal data.

b) Details of the categories of personal data collected, held, and processed by the Company; and the categories of data subject to which that personal data relates.

c) Details (and categories) of any third parties that will receive personal data from the Company.

d) Details of how long personal data will be retained by the Company; and

e) Detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data.

10. Privacy Impact Assessments

The Company shall carry out Privacy Impact Assessments when and as required under the Regulation.

11. The Rights of Data Subjects

The Regulation sets out the following rights applicable to individuals:

a) The right to be informed;
b) The right of access;
c) The right to rectification;
d) The right to erasure (also known as the 'right to be forgotten');
e) The right to restrict processing;
f) The right to data portability;
g) The right to object;

Rights with respect to automated decision-making and profiling.

12. Keeping Data Subjects Informed

12.1 The Company shall ensure that the following information is provided to every data subject when personal data is collected:

a) Details of the Company including, but not limited to, the identity of its Data Protection Officer;

b) The purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 21 of this Policy) and the legal basis justifying that collection and processing;

c) Where applicable, the statutory or contractual basis (including if appropriate the legitimate interests) upon which the Company is justifying its collection and processing of the personal data;

d) Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;

e) Where the personal data is to be transferred to one or more third parties, details of those parties;

f) Details of the length of time the personal data will be held by the Company (or, where there is no predetermined period, details of how that length of time will be determined);

g) Details of the data subject's rights under the Regulation;

h) Details of the data subject's right to withdraw their consent to the Company processing of their personal data at any time;

i) Details of the data subject's right to complain to the Information Commissioner's Office (the 'supervisory authority' under the Regulation);

j) Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it;

k) Details of any automated decision-making that will take place using the personal data (including but not limited to profiling), including information on how decisions will be made, the significance of those decisions and any consequences.

13. Data Subject Access

13.1 A data subject may make a subject access request ("SAR") at any time to find out more about the personal data which the Company holds about them. The Company is normally required to respond to SARs within one month of receipt.

13.2 All subject access requests received must be forwarded to the Company's data protection officer.

14. Rectification of Personal Data

14.1 If a data subject informs the Company's that personal data held by the Company is inaccurate or incomplete, requesting that it be rectified, the personal data in question shall be rectified, and the data subject informed of that rectification, within one month of receipt the data subject's notice.

15. Erasure of Personal Data

15.1 Data subjects may request that the Company erases the personal data it holds about them in the following circumstances:

a) It is no longer necessary for the Company to hold that personal data with respect to the purpose for which it was originally collected or processed;

b) The data subject wishes to withdraw their consent to the Company holding and processing their personal data;

c) The data subject objects to the Company holding and processing their personal data (and there is no overriding statutory, or contractual, or legitimate interest to allow the Company to continue doing so) (see Part 18 of this Policy for further details concerning data subjects' rights to object);

d) The personal data has been processed unlawfully;

e) The personal data needs to be erased in order for the Company to comply with a particular legal obligation;

15.2 Unless the Company has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request

16. Restriction of Personal Data Processing

16.1 Data subjects may request that the Company ceases processing the personal data it holds about them. If a data subject makes such a request, the Company shall retain only the amount of personal data pertaining to that data subject that is necessary to ensure that no further processing of their personal data takes place.

17. Data Portability

17.1 The Company processes personal data using automated means.

17.2 Where data subjects have given their consent to the Company to process their personal data in such a manner or the processing is otherwise required for the performance of a contract between the Company and the data subject, data subjects have the legal right under the Regulation to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers, e.g. other organisations).

17.3 To facilitate the right of data portability, the Company shall make available all applicable personal data to data subjects in the following formats:

a) Portable Document Format (PDF).

b) Extensible Mark-up Language (XML).

c) Text Delimited.

18. Objections to Personal Data Processing

18.1 Data subjects have the right to object to the Company processing their personal data based on legitimate interests (including profiling), direct marketing (including profiling), and processing for scientific and/or historical research and statistics purposes.

18.2 Where a data subject objects to the Company processing their personal data based on its legitimate interests, the Company shall cease such processing forthwith, unless it can be demonstrated that the Company's legitimate grounds for such processing override the data subject's interests, rights and freedoms; or the processing is necessary for the conduct of legal claims.

18.3 Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing forthwith.

18.4 Where a data subject objects to the Company processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the Regulation, 'demonstrate grounds relating to his or her particular situation'. The company is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

19. Automated Decision-Making

19.1 In the event that the company uses personal data for the purposes of automated decision-making and those decisions have a legal (or similarly significant effect) on data subjects, data subjects have the right to challenge to such decisions under the Regulation, requesting human intervention, expressing their own point of view, and obtaining an explanation of the decision from the company.

20. Profiling

Where the Company uses personal data for profiling purposes, the following shall apply:

a) Clear information explaining the profiling will be provided, including its significance and the likely consequences;

b) Appropriate mathematical or statistical procedures will be used;

c) Technical and organisational measures necessary to minimise the risk of errors and to enable such errors to be easily corrected shall be implemented; and

d) All personal data processed for profiling purposes shall be secured in order to prevent discriminatory effects arising out of profiling (see Parts 22 and 23 of this Policy for more details on data security).

21. Personal Data

Personal data may be collected, held, and processed by the Company; examples include but are not limited to:

a) Name

b) Address

c) Bank account details

d) Next of kin / emergency contact details

e) Medical records (company related) / GP contact

f) Email / phone numbers / communication methods

g) Driving licence / where applicable car related data (insurance)

h) Payroll / pension related data including any statutory payments and requested deductions (e.g. union subscription, court orders, student loans)

i) Photographs / video records

j) Training records

k) Accident records

l) CV / application forms

m) Current disciplinary / grievance records

n) Job title / career progression

o) Start date / contract of employment

p) Incentive schemes

q) Tax records

22. Data Protection Measures

The Company shall ensure that all its employees, agents, contractors, or other parties working on its behalf comply with the following when working with personal data:

a) All emails containing personal data must be encrypted using *DESlock (*provided by the Company);

b) Where any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. Hardcopies should be shredded, and electronic copies should be deleted securely using DESlock Shredder (provided by the Company).

c) Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;

d) Personal data may not be transmitted over a wireless network if there is a wired alternative that is reasonably practicable;

e) Personal data contained in the body of an email, whether sent or received, should be encrypted. If it is not possible to encrypt the contents it should be deleted;

f) Where Personal data is to be sent by facsimile transmission the recipient should be informed in advance of the transmission and should be waiting by the fax machine to receive the data;

g) Where Personal data is to be transferred in hardcopy form it should be passed directly to the recipient or sent using the appropriately secure method; this should be considered on a case by case basis;

h) No personal data may be shared informally and if an employee, agent, subcontractor, or other party working on behalf of the Company requires access to any personal data that they do not already have access to, such access should be formally requested from their senior manager or other relevant senior officer.

i) All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet or similar;

j) No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of the Group or not, without the authorisation of **Matthew Taylor or a Director.**

k) Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors or other parties at any time;

l) No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets and smartphones), whether such device belongs to the Group or otherwise without the formal written approval and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary.

m) All personal data stored electronically should be backed up daily with backups stored offsite. All files to be backed up should be encrypted using DESlock to ensure the contents of such backups are in an encrypted form;

n) All electronic copies of personal data should be stored securely using passwords and data encryption;

o) All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised.

p) Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Group, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;

23. Organisational Measures

The Company shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

a) All employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under the Regulation and under this Policy, and shall be provided with a copy of this Policy;

b) Only employees, agents, sub-contractors, or other parties working on behalf of the Group that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Company;

c) All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so;

d) All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised;

e) Methods of collecting, holding and processing personal data shall be regularly evaluated and reviewed;

f) The performance of those employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;

g) All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of the Regulation and this Policy by contract;

h) All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and the Regulation;

i) Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

24. Transferring Personal Data to a Country Outside the EEA

24.1 The Company may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the EEA.

24.2 The transfer of personal data to a country outside of the EEA shall take place only if one or more of the following applies:

a) The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data;

b) The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the European Commission; compliance with an approved code of conduct approved by a supervisory authority (e.g. the Information Commissioner's Office); certification under an approved certification mechanism (as provided for in he Regulation); contractual clauses agreed and authorised by the competent supervisory authority; or provisions inserted into administrative arrangements between public authorities or bodies authorised by the competent supervisory authority;

c) The transfer is made with the informed consent of the relevant data subject(s);

d) The transfer is necessary for the performance of a contract between the data subject and the Group (or for pre-contractual steps taken at the request of the data subject);

e) The transfer is necessary for important public interest reasons;

f) The transfer is necessary for the conduct of legal claims;

g) The transfer is necessary to protect the interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or

h) The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

25. Data Breach Notification

25.1 All personal data breaches must be reported immediately to the Company's data protection officer.

25.2 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the data protection officer must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.