Data Processing Agreement

Definitions and Interpretation

This document outlines the mutually agreed data processing agreement on which Marking Solutions Ltd, hereafter referred to as the Supplier, will provide to [Customer Name] hereafter referred to as the Client to undertake work in relation to the product and service requested from us, hereafter referred to as the Product.

Data Controller has the meaning given to that term (or 'controller') in Data Protection Laws;

Data Processor has the meaning given to that term (or 'processor') in Data Protection Laws;

Data Subject has the meaning in Data Protection Laws;

Data Subject Request means a request made by a Data Subject to exercise any rights under Data Protection Laws;

Data Protection Laws means any applicable law, regulation, direction, policy or rule relating to the processing, privacy, and use o
f Personal Data, as applicable to the Client, the Supplier and/or the services provided by the Supplier, including but not limited to :

(i) *the Data Protection Act 1998 and the Privacy and Electronic Communications (EC Directive) Regulations 2003, SI 2003/2426, and any laws or regulations implementing Directive 95/46/EC (Data Protection Directive) or Directive 2002/58/EC (ePrivacy Directive); and/or*

(ii) *the General Data Protection Regulation (EU) 2016/679 (GDPR), and/or any corresponding or equivalent national laws or regulations (Revised UK DP Law);*

Data Protection Losses means all liabilities and other amounts, including all: (a) costs (including legal costs), claims, demands, actions, settlements, interest, charges, procedures, expenses, losses and damages; (b) to the extent permitted by law: (i) administrative fines, penalties, sanctions, liabilities or other remedies imposed by a Supervisory Authority; (ii) compensation paid to a Data Subject; (iii) costs of compliance with investigations by a Supervisory Authority; and (iv) any loss of or corruption to the data of customers of the Client.

International Recipient has the meaning given in paragraph 6.1;

Personal Data has the meaning given in Data Protection Laws;

Personal Data Breach means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, any Protected Data;

Processing or process have the meanings given in Data Protection Laws;

Processing Instructions has the meaning given in paragraph 2.1.1;

Protected Data means Personal Data received from or on behalf of the Client, or otherwise obtained in connection with the performance of the Supplier's obligations;

Supervisory Authority means any local, national or multinational agency, department, official, parliament, public or statutory person or any government or professional body, regulatory or supervisory authority, board or other body responsible for administering Data Protection Laws;

1. Data Processor and Data Controller

1.1. The parties agree that, for the Protected Data, the Client shall be the Data Controller and the Supplier shall be the Data Processor.
1.2. The Supplier shall comply with all Data Protection Laws in connection with the processing of Protected Data and the exercise and performance of its respective rights and obligations under the Contract.
1.3. The Client shall comply with all Data Protection Laws in respect of the performance of its obligations under the Contract.

2. Instructions and details of processing

2.1. Insofar as the Supplier processes Protected Data on behalf of the Client, the Supplier:
2.1.1. unless required to do otherwise by law, shall (and shall ensure each person acting under its authority shall) process the Protected Data only on and in accordance with the Client's documented instructions as set out in this paragraph 2 and 0 (Data Processing Details), and as updated from time to time by the written agreement of the parties (Processing Instructions); and
2.1.2. if any applicable law requires it to process Protected Data other than in accordance with the Processing Instructions, shall notify the Client of any such requirement before processing the Protected Data (unless the applicable law prohibits such information on important grounds of public interest).
2.2. The processing to be carried out by the Supplier under the Contract shall comprise the processing set out in writing as part of the proposal or change requests, and such other processing as agreed by the parties in writing from time to time.
2.3. The Client undertakes to use the secure facilities provided by the Supplier to transfer all data to the Supplier and that the Supplier will transfer any data back to the Client utilising the same facilities.
2.4. The Client uses strong passwords and keeps them confidential in relation to systems and sites provided by the Supplier.

3. Technical and organisational measures

3.1. The Supplier shall implement and maintain, at its cost and expense, appropriate technical and organisational measures in relation to the processing of Protected Data by the Supplier:
3.1.1. Such that the processing will meet the requirements of Data Protection Laws and ensure the protection of the rights of Data Subjects;
3.1.2. so as to ensure a level of security in respect of Protected Data processed by it is appropriate to the risks that are presented by the processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed; and
3.1.3. without prejudice to paragraph 5.1, insofar as is possible, to assist the Client in the fulfilment of the Client's obligations to respond to Data Subject Requests relating to Protected Data.
3.2. Without prejudice to paragraph 3.1.2, the Supplier shall, in respect of the Protected Data processed by it under the Contract comply with the requirements regarding security of processing set out in Data Protection Laws.

4. Using staff and other processors

4.1. The Supplier shall not engage another Data Processor for carrying out any processing activities in respect of the Protected Data without ensuring compliance with Data Protection Laws. 4.2. The

Supplier shall ensure that all its personnel, representatives and subcontractors ('Agency Personnel') processing Protected Data are subject to a binding written contractual obligation with the Supplier to keep the Protected Data confidential (except where disclosure is required in accordance with applicable law).

4.3. Without prejudice to any other provision of paragraphs 1 to 10 (inclusive), the Supplier shall ensure that Agency Personnel processing Protected Data are reliable and have received adequate training on compliance with the Data Protection Laws applicable to the processing.

4.4.1 The processor should not engage another processor (a sub-processor) without the controller's prior specific or general written authorisation;

4.4.2 If a sub-processor is employed under the controller's general written authorisation, the processor should let the controller know of any intended changes and give the controller a chance to object to them;

4.4.3 If the processor employs a sub-processor, it must put a contract in place imposing the same data protection obligations on that sub-processor. This should include that the sub-processor will provide sufficient guarantees to implement appropriate technical and organisational measures in such a way that the processing will meet the UK GDPR's requirements. The wording of these obligations do not need to exactly mirror those set out in the contract between the controller and the processor, but should offer an equivalent level of protection for the personal data; and

4.4.4 The processor is liable to the controller for a sub-processor's compliance with its data protection obligations.

5. Assistance with the Client's compliance and Data Subject rights

5.1. The Supplier shall (at no cost to the Client):

5.1.1. Promptly record and then refer all Data Subject Requests it receives to the Client within three days of receipt of the request;

5.1.2. provide such information and cooperation and take such action as the Client requests in relation to a Data Subject Request, within the timescales required by the Client; and

5.1.3. not respond to any Data Subject Request or Complaint without the Client's prior written approval.

5.2. Without prejudice to paragraph 2.1, the Supplier shall, at its cost and expense, provide such information, co-operation and other assistance as the Client requires (taking into account the nature of processing and the information available to the Supplier) to the Client in ensuring compliance with the Client's obligations under Data Protection Laws, including with respect to:

5.2.1. security of processing;

5.2.2. data protection impact assessments (as such term is defined in Data Protection Laws);

5.2.3. prior consultation with a Supervisory Authority regarding high risk processing; and

5.2.4. any remedial action and/or notifications to be taken in response to any Personal Data Breach and/or Complaint, including (subject in each case to the Client's prior written authorisation) regarding any notification of the Personal Data Breach to Supervisory Authorities and/or communication to any affected Data Subjects.

6. International data transfers

6.1. The Supplier shall not transfer any Protected Data to any country outside the European Economic Area (EEA) or to any international organisation (an International Recipient) without the Client's prior written consent.

7. Records, information and audit

7.1. The Supplier shall maintain complete, accurate and up to date written records of all categories of processing activities carried out on behalf of the Client, containing such information as the Client may reasonably require on request in a timely manner.

7.2. The Supplier shall:
7.2.1. allow for and contribute to audits, including inspections, conducted by the Client or another auditor mandated by the Client for the purpose of demonstrating compliance by the Supplier with its obligations under Data Protection Laws; and
7.2.2. provide (and procure) reasonable access for the Client or such other auditor (where practicable) to the facilities, equipment, premises and sites on which Protected Data and/or the records referred to in paragraph 7.1 are held (in each case whether or not owned or controlled by the Supplier); provided that the Client gives the Supplier reasonable prior notice of such audit and/or inspection.
7.3. The Supplier shall promptly resolve, at its own cost and expense, all data protection and security issues discovered by the Client and reported to the Supplier that reveal a breach or potential breach by the Supplier of its obligations as defined in this document.

8. Breach notification

8.1. In respect of any Personal Data Breach, the Supplier shall:
8.1.1. notify the Client of the Personal Data Breach without undue delay (but in no event later than one working day after becoming aware of the Personal Data Breach); and
8.1.2. provide the Client without undue delay with such details as the Client reasonably requires regarding: (a) the nature of the Personal Data Breach; (b) any investigations into such Personal Data Breach; and (c) any measures taken, or that the Supplier recommends, to address the Personal Data Breach.
8.2. The Supplier shall promptly (and in any event within two working days) inform the Client if it receives a Complaint and provide the Client with full details of such Complaint.

9. Deletion or return of Protected Data and copies

9.1. The Supplier shall without delay, at the Client's written request, either securely delete or securely return all the Protected Data to the Client in such form as the Client reasonably requests after the earlier of:
9.1.1. the end of the provision of the relevant services related to processing; or
9.1.2. once processing by the Supplier of any Protected Data is no longer required for the purpose of the Supplier's performance of its relevant obligations under the Contract; and securely delete existing copies (unless storage of any data is required by law and, if so, the Supplier shall inform the Client of any such requirement).

10. Relationship with the Data Processing Agreement

10.1 Any claims against the Supplier or its affiliates under this DPA shall be brought solely against the entity that is a party to the Agreement. In no event shall any party limit its liability with respect to any individual's data protection rights under this DPA or otherwise. The Client further agrees that any regulatory penalties incurred by the Supplier in relation to the Customer Data that arise as a result of, or in connection with, the Client's failure to comply with its obligations under this DPA or any applicable Data Protection Laws shall count toward and reduce the Supplier's liability under the Agreement as if it were liable to the Customer under the Agreement.
10.2. This paragraph 10 is intended to apply to the allocation of liability for Data Protection Losses as between the parties, including with respect to compensation to Data Subjects, notwithstanding any provisions under Data Protection Laws to the contrary, except:
10.2.1. to the extent not permitted by law (including Data Protection Laws); and
10.2.2. that it does not affect the liability of either party to any Data Subject.

Signed on behalf of [Customer Name]

Signature:

Name:

Position:

Date:

Signed on behalf of Marking Solutions Ltd
Marking Solutions Ltd
12 Thurstin Way,
Gillingham,
Dorset,
SP8 4FN
Company No. : 10453100

Signature:

Name:

Position:

Date: