GDPR Statement & Data Processing Agreement

This Agreement dated XXXXXX is between:

(1)Rapid Mailing & Printing Ltd. registered at Oaklands House, London Road, East Grinstead, West Sussex, RH19 1PH and company registration number 9925356 (the Processor)

and

(2) xxxxx, registered at xxxxx and company registration number xxxxx (the Controller)

Whereas:

A) This Agreement is supplemental to any other separate agreement entered into between the parties and introduces further contractual provisions to ensure the Controller and the Processor comply with their respective obligations under the GDPR in respect of the Data Processing.

B) Recital 81 and Article 28of the GDPR place certain obligations upon a Controller to ensure that the Processor it engages under the terms of this Agreement provides sufficient guarantees in terms of: i) expert knowledge, ii) reliability and resources, iii) ability to implement technical and organisational measures which will meet the requirements of the GDPR including for the security of processing

C) The Controller must also take into account the specific tasks and responsibilities of the Processor under this Agreement in the context of the processing to be carried out and the risks to the rights and freedoms of the data subject. The Controller in this case may not be the original data owner but is acting on behalf of the data owner as a sub controller, and guarantees that a similar parallel agreement exists with the initial Controller to ensure that all data supplied is GDPR compliant

D) This Agreement exists to ensure that there are sufficient guarantees in place as required by the GDPR and that the processing complies with the obligations imposed on both the Controller and the Processor under the GDPR.

1. Definitions

"Data" shall mean [List the categories of the data that is being processed and the categories of data subjects this processing relates to]

“Data Subject” shall have the same meaning as set out in Article 4 (1) of the GDPR and means an identified or identifiable natural person

“EEA” means the European Economic Area – the 28 Member states of the European Union plus Iceland, Lichtenstein and Norway

“GDPR” means the General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and the Council

“Incident” has the same meaning as a personal data breach in Article 4 (12) of the GDPR and means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Data , transmitted, stored or otherwise processed under the terms of this Agreement

"Processing" shall mean any operation or set of operations which is/are performed upon Data , (whether or not by automatic means) including collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. Such processing may be wholly or partly by automatic means or processing otherwise than by automatic means of Data which form part of a filing system or one intended to form part of a filing system. A filing system shall mean any structured set of Data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographic basis."

2. Application

This Agreement shall apply to all Data processed from the date of this Agreement by the Processor on behalf of the Controller until the date of termination of this Agreement.

3. Purpose of Processing

a) The Processor shall process the Data it processes on behalf of the Controller, solely for the provision of direct mail and postage services in accordance with the written instructions of the Controller (including when making a transfer of personal data to countries outside the EEA) unless required to do by law. The Processor must inform the Controller of what processing the Processor is required to do so by law unless the Processor is prohibited under the relevant law from notifying the Controller of such processing. The Processor shall not process the Data for any other purpose except with the express written consent of the Controller.

b) The Controller confirms and warrants that the Processing of the Data, including the transfer of the Data to the Processor, has been and will continue to be carried out in accordance with the relevant provisions of the GDPR and does not violate the relevant provisions of the EEA country in which the Controller is established. Further that the data is fully compliant with GDPR on the basis of Consent/Legitimate Interest (delete one)

4. Duration of processing

The Processor shall process the Data for as long as this agreement for the provision of direct mail and postal services dated 25th May 2018 remains in full force and effect.

5. Type of Personal data

The Processor will process the following types of personal information

- personal details

- family details
- lifestyle and social circumstances
- goods and services
- financial details
- employment and education details
- details of complaints, incidents and grievances
- visual images, personal appearance and behaviour
- responses to surveys
- behavioural data
- profile data
- social media data
- tracking data from web activity

5. Categories of data subjects

The Processor will process information about the following categories of data subjects

- customers
- prospective customers
- complainants or their representatives
- subject of a complaint or their representatives
- individuals contacted when responding to a complaint or enquiry
- service providers

6. Security and Confidentiality of Data

a) The Processor and the Controller shall implement appropriate technical and organisational measures to ensure a level appropriate to the risks that are presented by the data processing in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal transmitted, stored or otherwise processed.

b) Both the Controller and Processor shall take into account the following when determining the measures:

i) the state of the art, and

ii) the cost of implementation of the measures, and

iii) the nature, scope context and purposes of processing, and

iv) the risk of varying likelihood and severity for the rights and freedoms of individual Data Subjects

c) The Controller and Processor agree that the security measures taken in accordance with Clause 6 (a) of this Agreement after assessment with the requirements of the GDPR are appropriate to protect Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the Processing involves the transmission of Data over a network, and against all other unlawful forms of Processing, and that these measures ensure a level of security appropriate to the risks presented by the Processing and the nature of the Data to be protected having regard to the state of the art and the cost of their implementation; shall ensure a level of security appropriate to the risk,

d) The measures taken shall include amongst others the following items, where appropriate, from the non- exhaustive list below:

i) the pseudonymisation and encryption of Data

II) the ability to ensure the ongoing confidentiality, integrity and availability and resilience of processing systems and services

III) the ability to restore the availability and access to Data in a timely manner in the event of a physical or technical Incident

iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

e) The Controller and the Processor may use adherence to an approved code of conduct as referred to by Article 40 of the GDPR or an approved certification mechanism as referred to in Article 42 as an element by which to demonstrate compliance with the requirements set out above in clause 6) (b) (c) and (d) of this Agreement

f). The Processor shall ensure that each of its employees, agents or subcontractors are made aware of its obligations with regard to the security and protection of the Data and shall require that they enter into binding obligations with the Processor in order to maintain the levels of security, protection and confidentiality provided for in this Agreement.

g). The Processor shall not divulge the Data whether directly or indirectly to any person, firm or company without the express consent of the Controller except to those of its employees, agents and subcontractors who are engaged in the processing of the Data and are subject to the binding obligations referred to in Clause 6 (e) of this Agreement above).

7. Incident Reporting

a) The Processor must have effective processes for the identification, management and reporting of Incidents. Any Incident, suspected or actual, involving the Controller's Data must be reported immediately to the Controller. An Incident may include but not be limited to:

- Security breach or fraud
- Misuse of relevant system storing Controller's Data

- Misuse, loss or corruption of the Controller's Data
- Unauthorised access to, use of, alteration, amendment or deletion of Controller's Data
- Physical security incident
- Any unapproved requirement to disclose Controller's Data to a third party

b) The Processor will be expected to promptly investigate any such Incident, provide status updates throughout the Incident, where appropriate cooperate with reasonable Controller requests during the management of the Incident or permit the Controller to support the management of the Incident, and send a written report to the Controller, describing the nature of the Incident, stating any control weaknesses discovered, and any actions taken/planned. A plan to agree any reasonable additional controls, either identified by the Processor or the Controller, to prevent or reduce the likelihood of a similar Incident must be agreed and monitored.

c) The Processor will assist the Controller in informing Data Subjects if there has been an Incident involving the Processor.

d) The Processor will assist the Controller in informing any relevant supervisory authority of an Incident.

8. Processor's appointment of a sub - processor

a) The Processor may engage a sub processor to process the Controller's Data, without the prior specific or general or written authorisation of the Controller.

b) If the Processor employs a sub – processor without the Controller's prior general written authorisation the Processor will ensure that all the provisions of the GDPR and this agreement are reflected within a parallel agreement.

c) The Processor shall ensure by written contract that any agent or sub-processor employed by the Processor to process Data to which this Agreement relates:

i) imposes the same contract terms as listed in Clause 6 – Security and Confidentiality of Data and Clause 7 Incident reporting of this Agreement on any agent or sub- processor [1]

ii) makes it clear that the Processor and not any agent or sub-processor will be liable to the Controller for the compliance of the agent or sub- processor with data protection law

f) The Processor will immediately inform the Controller of any Incident involving any of its' permitted sub-contractors or sub-processors in accordance with Clause 7 Incident reporting of this Agreement.

g) The Processor will assist the Controller in informing Data Subjects if there has been an Incident involving any of its' permitted sub-contractors or sub-processors in accordance with Clause 7 Incident reporting of this Agreement.

h) The Processor will assist the Controller in informing any relevant supervisory authority of an Incident.

9. Data Subjects rights

a) The Processor shall have appropriate technical and organisational means taking account of the nature of the Processing in so far as this is possible for the fulfilment of the Controller‘s obligation to respond to requests for exercising the following Data Subject’s rights :

i) information rights under Articles 13 and 14 of the GDPR

ii) right of access by the Data Subject under Article 15 of the GDPR

iii) right to rectification under Article 16 of the GDOR

iv) right to erasure under Article 17 of the GDPR

v) right to restriction of processing under Article 18 of the GDPR

vi) notification regarding the right of rectification and/or erasure of personal data and/or restriction of processing under Article 19 of the GDPR

vii) right to data portability under Article 20 of the GDPR

10. Assisting the Controller

a) The Processor will assist the Controller, taking into account the nature of the Processing and the information available to the Processor, to meet the Controller’s obligations

i) to keep Data secure in accordance with Article 32 of the GDPR

ii) to notify Incidents in accordance with Article 33 of the GDPR

iii) to advise Data Subjects when there has been an Incident in accordance with Article 34 of the GDPR

iv) to carry out data protection impact assessments (DPIAs) in accordance with Article 35 GDPR

v) to consult with the Controller’s supervisory authority where a DPIA indicates there is an unmitigated high risk in accordance with Article 36 of the GDPR

b) The Processor will immediately pass on any notices, requests or other communications from a Data Subject. The Processor will not act on any request from a Data Subject, without the full written authority of the Controller.

c) If a privacy impact assessment indicates that there is an unmitigated high risk to the rights and freedoms of the Data Subject, the Processor will assist the Controller in consulting with the relevant supervisory authority or authorities

11. Audit, inspections and legal processing

a) The Processor must provide the Controller with all the information that is needed to show that both the Processor and the Controller have met their obligations under Article 28 of the GDPR

b) The Processor must submit and contribute to audits and inspections conducted by the Controller or another auditor mandated by the Controller within reasonable provisions.

12. Processor's responsibilities and liabilities under the GDPR

a) The Processor is aware that it may be subject to enforcement action by any relevant data protection supervisory authority to which the Controller is subject under Article 58 (Powers of the supervisory authority) of the GDPR.

b) The Processor is aware that if it fails to meet its obligations as set out in this Agreement and under Article 83 (General conditions for imposing administrative fines) of the GDPR, it may be subject to an administrative fine.

c) The Processor is aware that if it fails to meet its obligations under GDPR, it may be subject to a penalty under Article 84 (Penalties) of the GDPR.

d) The Processor is aware that if it fails to meet its obligations under GDPR, it may have to pay compensation to individual Data Subjects under Article 82 (right to compensation and liability) of the GDPR.

e) The Processor will appoint a data protection officer, if required in accordance with Article 37 (designation of the data protection officer) of the GDPR.

f) The Processor will appoint (in writing) a representative within the European Union if required because it is not established in the European Union and the provisions of Article 3 (2) apply in accordance with Article 27 (representatives of controllers or processors not established in the Union) of the GDPR .

13. Liability

The Processor's liability to the Controller for any loss or damage of whatsoever nature suffered or incurred by the Controller or for any liability of the Controller to any other person for any loss or damage of whatsoever nature suffered or incurred by that person shall to the extent permitted by law not exceed the contract value, or the loss to the Controller, whichever is greater.

14. Termination

a) Subject to Clause 14 (b) either Party may terminate this Agreement upon giving 1 week's prior written notice to the other. Upon the date of termination of this Agreement, the Processor shall return or delete at the Controller's choice any Data received from the Controller to the Controller

The Processor shall not be obliged to return or delete any Data received from the Controller which has:

a) already been deleted in the normal course of events or

b) the Processor is required to retain by law.

b) Notwithstanding termination of this contract, the provisions of this Agreement shall survive the termination of this Agreement and shall continue in full force and effect for a period of 2 years from

the date of termination of the Agreement. The obligations contained in Clause 6 of this Agreement – Security and Confidentiality of Data – and Clause 7of this Agreement- Incident Reporting shall continue indefinitely.

15. Assignment

This Agreement shall not be transferred or assigned by either party except with the prior written consent of the other.

16. Jurisdiction

This Agreement shall be governed by and construed in accordance with the law of England and Wales and the parties shall submit to the exclusive jurisdiction of the Courts of England and Wales.

IN WITNESS WHEREOF, each of the Parties hereto has caused the Agreement to be executed by its duly authorised representative.

……	……
Signed for and on behalf of Rapid Mailing & Printing Ltd	Signed for and on behalf of xxxxx
……	……..
Name of person signing the Agreement	Name of person signing the Agreement
……..	……..
Position of person signing the Agreement	Position of person signing the Agreement
……..	……
Date of signature	Date of signature

Data & Marketing Association