101Smart Ltd

Data Processing Agreement

101Smart Ltd: May 2018

Data Processing Agreement

This Data Processing Agreement ("DPA") is entered into between (1) The Client stated in the Service Agreement as the "Data Controller" and (2) 101Smart Ltd acting as the Data Processor, Unit 15, Beech Avenue, Taverham, Norwich, NR8 6HW, Company No: 5294196 as "101"

Background

The Data Controller determines the purposes and methods of the processing of personal data which are described in the Processing Instruction [Annexe 1].

101 has agreed to provide the Products or Services defined within the Service Agreement which incorporates 101's applicable Terms and Conditions.

The parties wish to supplement the Service Agreement with this DPA to formalise the Terms and Conditions applicable to the processing of personal data.

The purpose of this DPA is to secure adequate safeguards with the respect to the protection of privacy and to ensure that the processing of personal data is in accordance with the Data Controller's and 101's legal obligations.

Agreement

In addition to this main body of the agreement, this DPA incorporates the following document:

Annex 1: Processing Instruction, details the operations to be carried out by 101 together with relevant contact details.

In the event that any provision of this DPA is inconsistent with any term(s) of the Service Agreement, this DPA shall prevail.

Definitions

For the purposes of this DPA, the expressions set out below have the following meanings:

Approved Purpose: The processing required to fulfil the purpose of the Service Agreement or as otherwise agreed between the Data Controller and 101 in writing.

Approved Territory: Within the United Kingdom (UK) or European Economic Area (EEA).

Data Subject: A living individual about whom the Data Controller holds personal data.

Personal Data: Has the same meaning as in Regulation 2016/679 of the European Parliament and the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

Personal Data Breach: Any loss, destruction, damage, inaccessibility, alteration or unauthorised access or disclosure of personal data or any other non-conformity with this DPA.

Products/Services: All products or services to be supplied by 101 under the Service Agreement.

Service Agreement: The service agreement for 101 Products/Services, which becomes effective upon the Data Controller's placement of an order and acceptance of the Terms and Conditions.

Technical Contact Point: The parties' technical representatives identified in the Processing Instructions given in Annexe 1.

General

This DPA governs 101's processing of the personal data it processes on behalf of the Data Controller to perform its obligations under the Service Agreement. 101 shall process the personal data only for the Approved Purpose and in accordance with applicable laws and this DPA.

The Data Controller retains the formal control of, and all ownership and rights to the personal data. 101 shall have no rights in or to the personal data other than the non-exclusive, revocable and time limited right to process the personal data for the Approved Purpose.

Approved Purpose of Processing

101 shall process the personal data only for the Approved Purpose. Any processing of the personal data for any other purpose is strictly forbidden and will be considered a material breach of this DPA.

Approved Locations of Processing

The processing of the personal data shall only take place in technological environments controlled by the Data Controller, 101 and its subcontractors in the Approved Territory. For the avoidance of doubt, processing includes accessing the personal data from remote locations.

Use of Subcontractors

The Data Controller accepts that 101 is entitled to use subcontractors. 101 shall ensure that any processing of the personal data by a subcontractor complies with the requirements set out under this DPA. This includes verifying that the security measures implemented by the subcontractor ensures at least the equivalent level of protection to that required of 101 under this DPA.

101 shall ensure that a data sharing agreement is entered into between 101 and any subcontractor before such subcontractor processes any personal data.

Processing of Personal Data in Other Territories

Where the processing of personal data does not take place within the UK or the EEA then a separate DPA must be agreed between the Data Controller and 101 whereby the Data Controller will approve or identify a subcontractor to carry out the processing. Prior to any processing in such territories, 101 shall enter into and/or shall procure that the subcontractor enters into (each a "data importer" under the EU Model Clauses), the EU Model Clauses with the Data Controller ("data exporter" under the EU Model Clauses), in addition to this DPA. In case of conflict between such EU Model Clauses entered into between the parties and this DPA, the EU Model Clauses will prevail.

101 is hereby authorised by the Data Controller to enter into the EU model Clauses agreements with any relevant subcontractor on the Data Controller's behalf for the above-mentioned purpose and for any relevant Approved Territory.

If the Data Controller is required to submit a copy of the executed EU Model Clauses to its local Data Protection Authority, 101 will submit a copy of the executed contract to the Data Controller for its submission.

For the avoidance of doubt, the requirement to ensure that the subcontractors enters into a data sharing agreement using the EU Model Clauses where so required does not relieve 101 from its obligations, including the obligation to ensure that the security measures adopted by the relevant subcontractor offer at least an equivalent level of protection to the Data Controller and the Data Subjects as the requirements imposed on 101 as set out in this DPA.

Technical and Organisational Security Measures

101 shall perform its obligations and actions under this DPA with all due skill, care and diligence.

101 shall use technical and organisational security measures appropriate to prevent the harm which might result from any unauthorised or unlawful processing, loss, destruction, damage, alternation to or

disclosure of the personal data and having regard to the nature of the personal data which is to be protected.

Should 101 become aware of any non-conformity with the security requirements set out above, either within its own or within the subcontractor's organisation, such non-conformity shall be notified to the Data Controller in accordance with the personal data Breach procedure set out below.

Secrecy

101 shall ensure that it and its employees maintain secrecy and security about any and all personal data and that the personal data is accessed by 101's employees on a need to know basis only.

The personal data shall be considered as confidential information belonging to the Data Controller and/or the Data Subject and shall be subject to confidential handling in accordance with the confidentiality undertakings agreed between the parties in this DPA or elsewhere.

Notification of Personal Data Breach

If 101 becomes aware of any personal data Breach, 101 shall without undue delay and within 24 hours at the latest, notify the Data Controller and fully cooperate to remedy the issue as soon as reasonably practicable. The notice shall contain the following information (if available):

- description of the personal data Breach including; the categories and number of Data Subjects concerned; summary of the incident that caused the personal data Breach; date and time of the relevant incident; the categories and number of data records concerned and the nature and content of the personal data affected;
- description of the circumstances of the personal data Breach (e.g. loss, theft, copying);
- description of recommended measures to mitigate any adverse effects of the personal data Breach;
- description of the likely consequences and potential risk that the personal data Breach may have towards the affected Data Subject(s);
- description of the measures proposed or taken by 101 and/or the sub-contractor, as applicable, to address the personal data Breach.

Notice must be sent by email to the Data Controller's Technical Contact Point identified in Annexe 1. 101's Technical Contact Point shall be available for expedient assistance to clarify and respond to any follow up questions that the Data Controller may have.

Depending of the nature of the personal data Breach the Data Controller may be obliged to make a report to the Data Protection Authority in the country it resides, in the UK this is the Information Commissioners Office. 101 shall, therefore, at the Data Controller's request, provide any other

information reasonably requested by the Data Controller to comply with the relevant data protection regulation and/or inquiries from the Data Protection Authority.

Other Notifications

101 shall:

- without undue delay and via email, notify the Data Controller of any planned changes in the technical, organisational or financial aspects of 101's provision of the Services or the organisation of 101 or its subcontractors and which might have an adverse effect on 101's or its subcontractors' ability or willingness to process the personal data in accordance with the instructions of the Data Controller or the requirements set out in this DPA.
- within five (5) calendar days and via email, notify the Data Controller if it receives a request from a Data Subject to have access to that person's personal data, or a complaint or request relating to the Data Controller's and/or its customers' obligations under relevant data protection laws.
- without undue delay, notify the Data Controller if it receives a request from the competent data protection authority or other competent governmental body requiring 101 or any of its subcontractors to grant the data protection authority or other applicable governmental body access to personal data. Such notice shall wherever possible, and to the extent permitted by applicable laws, be given prior to any disclosure by the Data Processor.

If 101 is required or requested by any law, regulation, or government or regulatory body to retain any documents or materials that it would otherwise be required to return or destroy, it shall, to the extent permitted by law, notify the Data Controller in writing of that retention, giving details of the documents or materials that it must retain. 101 shall not be in breach of its obligation to delete data with respect to the retained documents or materials; however, its obligation to report a breach shall continue to apply to them.

Any notifications shall be deemed to be delivered when submitted via email to the Data Controller's Technical Contact Point. 101's Technical Contact Point shall be available for expedient assistance to clarify and respond to any follow up questions that the Data Controller might have.

Breach of Agreement

101 shall ensure that any material breach is remedied as soon as possible.

Notwithstanding the above, the Data Controller can with immediate effect instruct 101 to suspend or terminate any further processing of the personal data upon the occurrence of any material breach of this DPA.

Obligation to Delete Data

Personal data shall not be stored for a longer period than it is necessary to carry out the original purpose for the processing.

101 permits the Data Controller to migrate personal data held by 101 and the Data Controller agrees to migrate any and all personal data prior to termination of the Service Agreement. 101 shall use reasonable commercial endeavours to permit the Data Controller to migrate data until expiry of the Service Agreement. Where the Service Agreement is terminated with immediate effect due to the Data Controller's breach of this DPA, 101 shall use reasonable commercial endeavours to permit the Data Controller to migrate data in the period of ten (10) days after such termination.

101 is not obligated to store any of the Data Controller's personal data after expiry of the Service Agreement. 101 shall no later than thirty (30) days after expiry of the Service Agreement effectively delete all personal data. For the purposes of this provision to effectively delete shall mean that the data is deleted in accordance with industry standards.

Without limiting the aforementioned, at any given time during the term of this DPA the Data Processor shall effectively delete personal data to the extent requested by the Data Controller's Technical Contact Point as stated in Annexe 1.

Term

This DPA is entered into when the Data Controller accepts this DPA. The acceptance of this DPA is made in connection with the Data Controller's acceptance of the Service Agreement. However, the provisions of this DPA will not become applicable before 25 May 2018. This DPA will remain in force until termination of the Service Agreement.

Survival of Clauses

Any provision of this DPA that expressly or by implication is intended to come into or continue in force on or after termination of this DPA shall remain in full force and effect.

To the extent the Data Controller needs to respond to enquiries from Data Protection Authorities or Data Subjects concerning how personal data has been processed under the Service Agreement and this DPA, 101 shall provide necessary assistance also after the expiry of this DPA.

For the avoidance of doubt the secrecy and security obligations set out herein, including the employees', consultants', and any others, obligation to keep personal data secret, shall survive the expiry or termination of this DPA.

Choice of Law and Dispute Resolution

This DPA shall be governed and construed in accordance with English Law. Any dispute, controversy or claim arising out of or in connection with this DPA shall be subject to the exclusive and final jurisdiction of the courts of England and Wales.

In the event that the Data Controller is located in a jurisdiction where judgments rendered by the above-mentioned courts cannot be enforced, any dispute, controversy or claim arising out of or in connection with this DPA shall be exclusively and finally settled by arbitration in accordance with the Arbitration Rules of The Arbitration Conciliation and Advisory Service (ACAS).