# SyncForce Data Processing Agreement

Effective date: May 25th 2018

The General Data Protection Regulation ("**GDPR**") takes effect on May 25, 2018. This regulation standardizes data privacy laws across the European Union (EU), and EU citizens are entitled to exercise their GDPR rights.

Customers of SyncForce B.V. ("**Syncforce**"), with its registered office in Eindhoven (5652 AR), The Netherlands, at Meerenakkerweg 1 07, within or outside of the EU are required to respond to requests from EU data subjects who ask to exercise their GDPR rights.

This SyncForce Data Processing Agreement ("**DPA**"), as applicable, reflects the parties' agreement with respect to the terms governing the Processing of Personal Data. This DPA is an amendment to the SyncForce Master Subscription Agreement ("**MSA**") and Terms of Use of SyncForce SurveyWorld ("**ToU**") and is effective upon its incorporation into the MSA. The term of this DPA shall follow the term of the MSA. In the event of any conflict between the DPA, MSA and ToU, the DPA will prevail.

## 1. Definitions

"Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data and in this case is a customer of Syncforce.

"Data Protection Law" means all applicable legislation relating to data protection and privacy including without limitation the EU Data Protection Regulation 2016/679, together with any national implementing laws in any Member State of the European Union or, to the extent applicable, in any other country, as amended, repealed, consolidated or replaced from time to time. The terms "process", "processes" and "processed" will be construed accordingly.

"Data Subject" means the individual to whom Personal Data relates.

"GDPR" means the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

"Instruction" means the written, documented instruction, issued by Controller to Processor, and directing the same to perform a specific action with regard to Personal Data (including, but not limited to, depersonalizing, blocking, deletion, making available).

"Personal Data" means any information relating to an identified or identifiable individual where such information is contained within Customer Data and is protected similarly as personal data or personally identifiable information under applicable Data Protection Law.

"Personal Data Breach" means a breach of security leading to the accidental or unlawful

destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

"Processing" means any operation or set of operations which is performed on Personal Data, encompassing the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction or erasure of Personal Data.

"Processor" means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller and in this case is Syncforce.

**2. Details of the Processing**

a. Categories of Data Subjects. Controller's Contacts and other end users including Controller's employees, contractors and collaborators.

b. Types of Personal Data. Name and email address of end users. Other categories of Personal Data can be processed if Surveyworld's customers ask their customers for other information than stated above, such as gender, address and language.

c. Subject-Matter and Nature of the Processing. The subject-matter of Processing of Personal Data by Processor is the provision of the services to the Controller that involves the Processing of Personal Data. Personal Data will be subject to those Processing activities as may be specified in the Agreement and an Order.

d. Purpose of the Processing. Personal Data will be Processed for purposes of providing the services set out and otherwise agreed to in the MSA and any applicable Order.

e. Duration of the Processing. Personal Data will be Processed for the duration of the MSA, subject to Section 4 of this DPA.

**3. Customer Responsibility**

Within the scope of the DPA and in its use of the services, Controller shall be solely responsible for complying with the statutory requirements relating to data protection and privacy, in particular regarding the disclosure and transfer of Personal Data to the Processor and the Processing of Personal Data. For the avoidance of doubt, Controller's instructions for the Processing of Personal Data shall comply with the Data Protection Law. This DPA is Customer's complete and final instruction to SyncForce in relation to Personal Data and that additional instructions outside the scope of DPA would require prior written agreement between the parties. Instructions shall initially be specified in the DPA and may, from time to time thereafter, be amended, amplified or replaced by Controller in separate written instructions (as individual instructions).

Controller shall inform Processor without undue delay and comprehensively about any errors or irregularities related to statutory provisions on the Processing of Personal Data.

**4. Obligations of Processor**

a. Compliance with Instructions. The parties acknowledge and agree that Customer is the Controller of Personal Data and SyncForce is the Processor of that data. Processor shall collect, process and use Personal Data only within the scope of Controller's Instructions. If the Processor believes that an Instruction of the Controller infringes the Data Protection Law, it shall immediately inform the Controller without delay. If Processor cannot process Personal Data in accordance with the Instructions due to a legal requirement under any applicable European Union, Processor will (i) promptly notify the Controller of that legal requirement before the relevant Processing to the extent permitted by the Data Protection Law; and (ii) cease all Processing (other than merely storing and maintaining the security of the affected Personal Data) until such time as the Controller issues new instructions with which Processor is able to comply. If this provision is invoked, Processor will not be liable to the Controller under the DPA for any failure to perform the applicable services until such time as the Controller issues new instructions in regard to the Processing.

b. Security. Processor shall take the appropriate technical and organizational measures – having regard to the Data Protection Legislation, the state of the art in the industry and the cost of their implementation – to adequately protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data. These measures are described in Exhibit 3 of this DPA and will comply with generally accepted security standards. In case of a security incident, Processor will report the incident to Controller. Processor will cooperate with Controller, if necessary, to inform the Data Subject about the security incident.

Upon Controller's request, Processor shall provide a current Personal Data protection and security programme relating to the Processing hereunder.

c. Confidentiality. Processor shall ensure that any personnel whom Processor authorizes to process Personal Data on its behalf is subject to confidentiality obligations with respect to that Personal Data.
The undertaking to confidentiality shall continue after the termination of the above-entitled activities.

d. Personal Data Breaches. Processor will notify the Controller as soon as practicable after it becomes aware of any Personal Data Breach affecting any Personal Data. At the Controller's request, Processor will report the nature of the Data Breach, the probable consequences of the Data Breach for the (access to the) Personal Data affected and any measures Processor has or will take(n) to address these consequences, to end the Data Breach and to prevent it from happening again. At Controller's request, Processor will promptly provide the Controller with all reasonable assistance necessary to enable the Controller to notify relevant Personal Data Breaches to competent authorities and/or affected Data Subjects, if Controller is required to do

so under the Data Protection Law. Controller will compensate any costs of Processor regarding such cooperation.

e. Data Subject Requests. Processor will provide reasonable assistance, including by appropriate technical and organizational measures and taking into account the nature of the Processing, to enable Controller to respond to any request from Data Subjects seeking to exercise their rights under the Data Protection Law with respect to Personal Data (including access, rectification, restriction, deletion or portability of Personal Data, as applicable), to the extent permitted by the law. If such request is made directly to Processor, Processor will promptly inform Controller and will advise Data Subjects to submit their request to the Controller. Controller shall be solely responsible for responding to any Data Subjects' requests. Controller shall reimburse Processor for the costs arising from this assistance. Procedure for controller to respond to these requests are described in Exhibit 1.

f. Sub-Processors. Processor shall be entitled to engage sub-Processors to fulfil Processor's obligations defined in the DPA only with Controller's written consent. For these purposes, Controller consents to the engagement as sub-Processors of Processor's affiliated companies and the third parties listed in Exhibit 2.

Where Processor engages sub-Processors, Processor will enter into a contract with the sub-Processor that imposes on the sub-Processor the same obligations that apply to Processor under this DPA.

Where the sub-Processor fails to fulfil its data protection obligations, Processor will remain liable to the Controller for the performance of such sub-Processors obligations.

The provisions shall mutually apply if the Processor engages a sub-Processor in a country outside the European Economic Area ("EEA") not recognized by the European Commission as providing an adequate level of protection for personal data. If, in the performance of this DPA, SyncForce transfers any Personal Data to a sub-processor located outside of the EEA, SyncForce shall, in advance of any such transfer, ensure that a legal mechanism to achieve adequacy in respect of that processing is in place.

g. Data Transfers. Controller acknowledges and agrees that, in connection with the performance of the services under the DPA, Personal Data will be transferred to SyncForce in The Netherlands.

h. Deletion or Retrieval of Personal Data. Other than to the extent required to comply with Data Protection Law, following termination or expiry of the DPA, Processor will delete all Personal Data (including copies thereof) processed pursuant to this DPA. If Processor is unable to delete Personal Data for technical or other reasons, Processor will apply measures to ensure that Personal Data is blocked from any further Processing.

Controller shall, upon termination or expiration of the DPA and by way of issuing an Instruction, stipulate, within a period of time set by Processor, the reasonable measures to return data or to delete stored data. Any additional cost arising in connection with the return or deletion of Personal Data after the termination or expiration of the DPA shall be borne by Controller.

i. Data protection impact assessment. In the event that Controller is obliged to do a DPIA pursuant to the Data Protection Legislation, Processor will assist Controller upon request. If the PIA indicates that the processing would result in a high risk, Processor shall assist the Controller upon request with consulting the supervisory authority.

j. Processor makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in this Article and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.
enables Controller to review compliance of Processor with this DPA via independent auditors and at the cost of Controller, without the use of any company confidential data of Processor and without disturbing the operations of Processor. If the review shows that Processor does not fully comply with its obligations under this DPA, Processor shall undo and/or repair the shortcomings identified by the review as soon as reasonably possible.
The aforesaid review will take place once a year at a maximum, unless there is real evidence to suggest that Processor does not comply with its obligations under this DPA. Processor shall provide Controller with all information reasonably necessary to perform the audit.
Processor shall immediately inform Controller if, in its opinion, an instruction infringes the Data Protection Legislation.

k. The controller and the processor and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks.

## 5. Liability and indemnification

a. Controller shall be solely responsible for determining the purposes for which and the manner in which the Personal Data are, or are to be, Processed by Controller. Controller is liable towards the Data Subjects(s) for the damage suffered as a result of any breach of the obligations referred to this DPA, notwithstanding the obligations of Processor arising from the MSA and this DPA. The liability of Processor towards a Data Subject shall be limited to the Processing operated by Processor under this DPA.

b. Controller shall reimburse all damage that Processor suffers resulting from any shortcoming by Controller of its obligations under this DPA to a maximum as set out in the MSA in article 10.1.

c. Controller shall indemnify Processor against any claims of third parties regarding the performance of this DPA except if and insofar as Controller proves that the damage was caused by an attributable shortcoming of Processor in the performance of this DPA.

d. Processor shall be liable for the damage caused by processing only where it has not complied with obligations of the Data Protection Legislation specifically directed to Processors or where it has acted outside or contrary to lawful instructions of the controller.

e. Any agreed limitation of liability in the MSA shall be applicable to any liability of Processor resulting from this DPA.

## Exhibit 1 – Who are SyncForce's sub-processors?

SyncForce maintains an up-to-date list of the names and locations of all sub-processors used for hosting or other processing of Personal Information, which can be found underneath.

1. XS4ALL Datacenter DC2, Barbara Strozzilaan 251, 1083 HN Amsterdam, The Netherlands
2. XS4ALL Datacenter Oude meer, Fokkerweg 300, 1438 BG Oude Meer, The Netherlands
3. SyncForce Meerenakkerweg 1.07, 5652 AR Eindhoven, The Netherlands

## Exhibit 2 – Technical and organizational security measures

The technical and organizational security procedures and measures shall comply with applicable and generally accepted security standards. The security measures to be taken by Processor will be the following (or comparable to these measures):

1. implemented security policy, updating and implementing the updated security policy;
2. implemented code of conduct;
3. confidentiality clause in employment contracts;
4. intruder alarm;
5. secure method for storage of data files;
6. logical access controls with the help of what people know, such as password or personal access code;
7. physical access controls with the help of what people carry, such as a security pass;
8. control on assigned rights;
9. logging and controlling the access to the system (including monitoring signs of unauthorised access to the Personal Data);
10. data access control: ensuring that persons entitled to use a Personal Data Processing system gain access only to such Personal Data as they are entitled to accessing in accordance with their access rights, and that, in the course of Processing or use and after storage, Personal Data cannot be read, copied, modified or deleted without authorization
11. recovery measures;
12. encryption of Personal Data during electronic transfer to external parties;
13. compliance with the confidentiality clause of this DPA; and

14. appointing a reasonably limited number of persons charged with the Processing of Personal Data and authorized to access the Personal Data, which persons will be explicitly entitled only to perform the operations necessary to fulfil the obligations of the Services Agreement.
15. ensuring that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media, and that the target entities for any transfer of Personal Data by means of data transmission facilities can be established and verified (data transfer control);
16. ensuring that Personal Data is Processed solely in accordance with the Instructions (control of instructions);
17. ensuring that Personal Data is protected against accidental destruction or loss (availability control).