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.
SyncForce & SurveyWorld customers 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"), that includes the Standard Contractual Clauses adopted by the European Commission, 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 and is effective upon its incorporation into the MSA, The term of this DPA shall follow the term of the MSA.

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.

"Data Protection Law" means all applicable legislation relating to data protection and privacy including without limitation the EU Data Protection Directive 95/46/EC and all local laws and regulations which amend or replace any of them, including the GDPR, 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laws in any Member State of the European Union or, to the extent applicable, in any other country, as amended, repealed, consolidated or replaced from time to time.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.

"Standard Contractual Clauses" means the clauses attached hereto as Exhibit 1 pursuant to the European Commission's decision (C(2010)593) of 5 February 2010 on Standard Contractual Clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

2. Details of the Processing

a. Categories of Data Subjects. Controller's Contacts and other end users including Controller's employees, contractors, collaborators, customers, prospects, suppliers and subcontractors. Data Subjects also include individuals attempting to communicate with or transfer Personal Data to the Controller's end users.

b. Types of Personal Data. Contact Information, the extent of which is determined and controlled by the Customer in its sole discretion, and other Personal Data such as navigational data (including website usage information), email data, system usage data, application integration data, and other electronic data submitted, stored, sent, or received by end users via the Subscription Service.

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 Agreement and any applicable Order.

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

3. Customer Responsibility

Within the scope of the Agreement 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 Agreement 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 Agreement 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 to adequately protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data. Such measures include, but are not be limited to:

i. the prevention of unauthorized persons from gaining access to Personal Data Processing systems (physical access control),

ii. the prevention of Personal Data Processing systems from being used without authorization (logical access control),

iii. 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 (data access control),

iv. 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),

v. ensuring that Personal Data is Processed solely in accordance with the Instructions (control of instructions),

vi. ensuring that Personal Data is protected against accidental destruction or loss (availability control).

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 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.

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 Agreement 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 Agreement, 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 Agreement, 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 Agreement 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 Agreement shall be borne by Controller.

Exhibit 1

Managing Personal Information

Customers can be either individual SyncForce and SurveyWorld users or organizations who own a SyncForce or SurveyWorld account with multiple users. SyncForce & SurveyWorld customers can view, edit, delete, and download a lot of personal data directly.

Managing Personal Information of Users

SyncForce & SurveyWorld users need to contact their Customer administrator and request the appropriate personal information request action.

Process regarding the SyncForce Solution

Users or former users can request what personal data is stored in SyncForce by asking this to the SyncForce customer. SyncForce customers are required to respond to requests from EU data subjects who ask to exercise their GDPR rights. As a data processor, SyncForce is not responsible for handling these requests on behalf of customers.

How to view and download personal data in SyncForce (only when authorized).
View user data: Go to “Manage Contact & Users”, select “Users and Rights”, select “Users”. Find the user and all user data is presented. In case the user would like to be erased, you can update the personal information and anonymize this user.
Download user data: Go to “Manage Contact & Users”, select “Users and Rights”, select “Export & Reports”. Select the needed report (Channel contact export or employee export).
If needed request a new one or download the latest one available.

Process regarding SurveyWorld

Within the User Profile section the user themselves can view and change their user information and a SurveyWorld Customer Administrator can login and see all users they manage. They can delete the user and update the information of the user in case you want to anonymize the user information.

Managing Personal Information of SurveyWorld Respondents

Managing Survey Response Data

SurveyWorld Customers are required to respond to requests from EU data subjects who ask to

exercise their GDPR rights. As a data processor, SyncForce is not responsible for handling these requests on behalf of customers.

SurveyWorld Respondents

Survey respondents and panelists are people that answered a survey sent by a SyncForce customer. You should contact the Customer who is responsible for editing, deleting, or giving you a copy of your responses.

Respondents should try to track down the following information before contacting the Customer:

- Email sender first name and last name in the email invitation;
- Survey link or web page you used to take the survey;
- Approximate date and time you took the survey;
- Your name and email address;
- Any response you provided that can be used to identify you.

In case a respondent can't track the Customer Contact he/she can contact SyncForce with the above mentioned information via privacy [@] syncforce.com

Since SyncForce is not the data controller of response data, we can't directly handle these requests, but we'll do our best to identify and put you in contact with the customer.

Unsubscribe from SurveyWorld

If you as a respondent want to unsubscribe from SurveyWorld you can click here (https://www.surveyworld.net/sw/surveys/unsubscription.asp)

SurveyWorld Administrators can view, delete or make anonymous the Respondent information following these steps:

Edit, View and export Respondent information:
Based on the survey code go to the survey and select "Results", select "Participants" and search for the email address of the Respondent. Click on the last name of this person and a screen opens where you can see all personal information of the respondent and his/her results. Also there is a printer icon above where you can print this data (for example as an pdf file).
In a running or a planned survey you can make the data anonymous by going to the participant and personal information. In a closed survey, the survey can be deleted (but then all data is deleted). In case you want to anonymize 1 or more respondents please contact SyncForce at: privacy [@] syncforce.com.

In case all personal information needs to be erased of 1 respondent, Customer can send a request to privacy [@] syncforce.com

Exhibit 2

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.

- KPN, Xs4all
- Pingdom
- Mailjet
- Google Analytics
- Leadboxer
- Gdrive
- Dropbox
- Ionbiz
- zendesk
- Matomo
- Acterus

Exhibit 3 Technical and organizational security measures

Definitions

A. Data exporter

The data exporter is the Customer, as defined in the HubSpot Customer Terms of Service ("Agreement").

B. Data importer

The data importer is HubSpot, Inc., a global provider of inbound marketing and sales software.

C. Data subjects

Categories of data subjects set out under Section 2 of the Data Processing Agreement to which the Clauses are attached.

D. Categories of data

Categories of personal data set out under Section 2 of the Data Processing Agreement to which the Clauses are attached.

E. Special categories of data (if appropriate)

The parties do not anticipate the transfer of special categories of data.

Description of the technical and organizational security measures implemented by the data importer:

SyncForce currently observes the security practices notwithstanding any provision to the contrary otherwise agreed to by data exporter, SyncForce may modify or update these practices at its discretion provided that such modification and update does not result in a material degradation in the protection offered by these practices. All capitalized terms not otherwise defined herein shall have the meanings as set forth in the Agreement.

a) Access Control

i) Preventing Unauthorized Product Access

Outsourced processing: SyncForce hosts its Service with outsourced cloud infrastructure providers. Additionally, SyncForce maintains contractual relationships with vendors in order to provide the Service in accordance with our Data Processing Agreement. SyncForce relies on contractual agreements, privacy policies, and vendor compliance programs in order to protect data processed or stored by these vendors.

Physical and environmental security: SyncForce hosts its product infrastructure with multi-tenant, outsourced infrastructure providers. The physical and environmental security controls are audited for SOC 2 Type II and ISO 27001 compliance, among other certifications.

Authentication: SyncForce implemented a uniform password policy for its customer products. Customers who interact with the products via the user interface must authenticate before accessing non-public customer data.

Authorization: Customer data is stored in multi-tenant storage systems accessible to Customers via only application user interfaces and application programming interfaces. Customers are not allowed direct access to the underlying application infrastructure. The authorization model in each of SyncForce's products is designed to ensure that only the appropriately assigned individuals can access relevant features, views, and customization options. Authorization to data sets is performed through validating the user's permissions against the attributes associated with each data set.

Application Programming Interface (API) access: Public product APIs may be accessed using an API key or through Oauth authorization.

ii) Preventing Unauthorized Product Use

SyncForce implements industry standard access controls and detection capabilities for the internal networks that support its products.

Access controls: Network access control mechanisms are designed to prevent network traffic using unauthorized protocols from reaching the product infrastructure. The technical measures implemented differ between infrastructure providers and include Virtual Private Cloud (VPC) implementations, security group assignment, and traditional firewall rules.

Static code analysis: Security reviews of code stored in SyncForce's source code repositories is performed, checking for coding best practices and identifiable software flaws.

Penetration testing: SyncForce maintains relationships with industry recognized penetration testing service providers for one annual penetration test. The intent of the penetration tests is to identify and resolve foreseeable attack vectors and potential abuse scenarios.

iii) Limitations of Privilege & Authorization Requirements

Product access: A subset of SyncForce's employees have access to the products and to customer data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support, to troubleshoot potential problems, to detect and respond to security incidents and implement data security. Access is enabled through "just in time" requests for access; all such requests are logged.

b) Transmission Control

In-transit: SyncForce makes HTTPS encryption (also referred to as SSL or TLS) available on every one of its login interfaces and for free on every customer site hosted on the SyncForce products. SyncForce's HTTPS implementation uses industry standard algorithms and certificates.

At-rest: SyncForce stores user passwords following policies that follow industry standard practices for security. With effect 25 May 2018, SyncForce has implemented technologies to ensure that stored data is encrypted at rest.

c) Input Control

Detection: SyncForce designed its infrastructure to log extensive information about the system behavior, traffic received, system authentication, and other application requests. Internal systems aggregated log data and alert appropriate employees of malicious, unintended, or anomalous activities. SyncForce personnel, including security, operations, and support personnel, are responsive to known incidents.

Response and tracking: SyncForce maintains a record of known security incidents that includes description, dates and times of relevant activities, and incident disposition. Suspected and confirmed security incidents are investigated by security, operations, or support personnel; and appropriate resolution steps are identified and documented. For any confirmed incidents, SyncForce will take appropriate steps to minimize product and Customer damage or unauthorized disclosure.

Communication: If SyncForce becomes aware of unlawful access to Customer data stored within its products, SyncForce will: 1) notify the affected Customers of the incident; 2) provide a description of the steps SyncForce is taking to resolve the incident; and 3) provide status updates to the Customer contact, as SyncForce deems necessary. Notification(s) of incidents, if any, will be delivered to one or more of the Customer's contacts in a form SyncForce selects, which may include via email or telephone.

d) Availability Control

Infrastructure availability: The infrastructure providers use commercially reasonable efforts to ensure a minimum of 99.95% uptime. The providers maintain a minimum of N+1 redundancy to power, network, and HVAC services.

Fault tolerance: Backup and replication strategies are designed to ensure redundancy and fail-over protections during a significant processing failure. Customer data is backed up to multiple durable data stores and replicated across multiple availability zones.

Online replicas and backups: Where feasible, production databases are designed to replicate data between no less than 1 primary and 1 secondary database. All databases are backed up and maintained using at least industry standard methods.

SyncForce's products are designed to ensure redundancy and seamless failover. The server instances that support the products are also architected with a goal to prevent single points of failure. This design assists SyncForce operations in maintaining and updating the product applications and backend while limiting downtime.