

DATA PROCESSING AGREEMENT

Revision Date: November 2, 2020

This Data Processing Agreement (“DPA”) reflects the parties’ agreement with regard to the Processing of Personal Data by or on behalf of Customer in connection with the Services under the Agreement.

This DPA is supplemental to, and forms an integral part of, the Agreement and is effective upon its incorporation into the Agreement, as specified in the Agreement, an Order Form, or a mutually executed amendment. If necessary, this DPA can be printed out by Customer and executed in counterparts and/or electronic signature. In case of a conflict or inconsistency with the terms of the Agreement, this DPA will take precedence over the terms of the Agreement to the extent of such conflict or inconsistency. For the purposes of this DPA, unless otherwise stated, all defined terms shall have the meanings given to them in accordance with the Agreement.

1. DEFINITIONS.

“**Agreement**” means, as applicable, the services or subscription agreement between WorldAPP, Inc. (hereinafter “FORM.com”) and Customer including, without limitation, the applicable Master Services Agreement, Terms of Use or Terms and Conditions of Subscription.

“**California Personal Information**” means Personal Data that is subject to the protection of the CCPA.

“**CCPA**” means California Civil Code Sec. 1798.100 et seq. (also known as the California Consumer Privacy Act of 2018).

“**Consumer**”, “**Business**”, “**Sell**” and “**Service Provider**” will have the meanings given to them in the CCPA.

“**Customer**” means the entity that executed the Agreement together with Affiliates, whether authorized to use the Services by Customer pursuant to the Agreement or Affiliates that have signed Order Forms.

“Customer Data” means new and modified information and data generated through Authorized Users of the Services including content of form questions (including the associated answers), documents, forms, user identification, all responses and data collected, and reporting of such responses and data.

“Data Protection Laws” means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland, the United Kingdom and the United States and its individual states (including the CCPA), applicable to the Processing of Personal Data under the Agreement.

“Data Subject Request” means a request or complaint from a Data Subject in relation to the individual’s Personal Data including any request to exercise such individual’s rights under Data Protection Laws.

“Data Subject” means the identified or identifiable person to whom Personal Data relates.

“GDPR” means 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 and repealing Directive 95/46/EC (General Data Protection Regulation).

“Instructions” means the written, documented instructions issued by Customer to FORM.com, and directing the same to perform a specific or general 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, personal information or personally identifiable information under applicable Data Protection Laws.

“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 by FORM.com and/or FORM.com’s Sub-Processors in connection with the provision of the Services. A Personal Data Breach will not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

“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.

“Services” means subscription, professional or related services provided to Customer by FORM.com pursuant to the terms of an applicable Agreement.

“Sub-Processor” means any service provider engaged by FORM.com or FORM.com Affiliates to assist in fulfilling FORM.com’s obligations with respect to the provision of the Services under the Agreement. Sub-Processors may include third parties or FORM.com Affiliates but will exclude any FORM.com employee, independent contractor or consultant.

“FORM.com” means WorldAPP, Inc. or Designlogic Ltd.

2. CUSTOMER RESPONSIBILITIES.

- a. **Compliance with Laws.** In Customer’s use of the Services, Customer will be responsible for complying with all requirements that apply to it under Data Protection Laws with respect to its Processing of Personal Data and the Instructions it issues to FORM.com. Without limiting the foregoing, Customer shall be solely responsible for the accuracy, quality, and legality of the Customer Data and the means the Customer Data was acquired. Customer shall be further solely responsible for complying with all requirements under Data Protection Laws for the Processing of the Personal Data, ensuring Customer has the right to transfer, or provide, access to, the Personal Data to WordApp for Processing in accordance with the terms of the Agreement and this DPA, and ensuring the Customer’s Instructions to FORM.com regarding the Processing of Personal Data comply with applicable laws, including Data Protection Laws.
- b. **Customer Instructions.** Customer agrees that the Agreement (including this DPA, SOWs or Order Forms), together with Customer’s use of the Services in accordance with the Agreement, constitute Customer’s complete and final Instructions to FORM.com in relation to the Processing of Personal Data, and additional instructions outside the scope of the Instructions shall require prior written agreement between FORM.com and Customer.
- c. **Data Transfers.** Customer acknowledges and agrees that FORM.com may access and Process the Personal Data as necessary to provide the Services in accordance with the Agreement, and in particular, that Personal Data will be transferred to and Processed by FORM.com in the United States and to other jurisdictions where FORM.com Affiliates and Sub-Processors have operations.

3. FORM.COM OBLIGATIONS

- a. **Limitation of Access.** FORM.com will ensure that FORM.com's access to Personal Data is limited to those personnel performing Services in accordance with the Agreement.
- b. **Compliance with Laws.** Within the scope of the Agreement, FORM.com will be responsible for complying with all requirements that apply to it under applicable Data Protection Laws with respect to its Processing of Customer's Personal Data. FORM.com, upon request by Customer, will provide Customer with reasonable assistance, at Customer's expense, in ensuring its compliance with the applicable Data Protection Laws taking into account the nature of processing and information available to FORM.com. FORM.com is not responsible for compliance with any Data Protection Laws applicable to Customer or Customer's industry that are not generally applicable to FORM.com.
- c. **Compliance with Instructions.** FORM.com will Process Personal Data for the purposes described in this DPA or otherwise agreed within the scope of Customer's lawful Instructions (except to the extent required by applicable law), including transfers of Personal Data to a third country or an international organization.
- d. **Demonstration of Compliance.** FORM.com will make available to Customer all information reasonably necessary to demonstrate compliance with this PDA and allow for audits in order to assess compliance with this PDA, provided that such audits shall take place no more than once per calendar year during the Term and shall be subject to the confidentiality obligations set forth in the Agreement and to agreed-to specifics regarding timing, scope and duration of the audit.
- e. **Confidentiality.** FORM.com will ensure that any personnel engaged by FORM.com in the Processing of Personal Data are subject to appropriate confidentiality obligations (whether a contractual or statutory obligation).
- f. **Security.** FORM.com will maintain appropriate technical and organizational measures for the protection of Personal Data from Personal Data Breaches including security incident management policies and procedures set forth in Schedule 2 attached hereto ("Security Measures"). FORM.com will regularly monitor compliance with such Security Measures. FORM.com may modify or update the Security Measures at its discretion provided that such modification or update does not result in a material degradation in the protection offered by the Security Measures.
- g. **Personal Data Breaches.** FORM.com will promptly notify Customer after it becomes aware of any Personal Data Breach and will provide timely information relating to the Personal Data Breach as it becomes known or reasonably requested by Customer. FORM.com will make reasonable efforts to identify the cause of such Personal Data Breach and take those steps as FORM.com deems

necessary and reasonable to remediate the cause of such Personal Data Breach to the extent the remediation is within FORM.com's reasonable control. The obligations herein shall not apply to incidents that are caused by Customer or Customer's Authorized Users.

- h. Return or Deletion of Personal Data. Through the Services, Customer is provided with a number of controls that can be used to retrieve, correct, delete or restrict Personal Data, which Customer can use to assist it in connection with its obligations under Data Protection Laws. To the extent applicable, FORM.com will return or delete all Customer Data (including Personal Data) Processed pursuant to this DPA on termination or expiration of the Agreement in accordance with the procedures and timeframes set out in the Agreement, except to the extent FORM.com is required by applicable law to retain any Customer Data, or to Customer Data archived on back-up systems as described in the Agreement.
- i. Other Assistance. FORM.com, upon Customer's request, will provide Customer with reasonable assistance to enable Customer to fulfill its obligations concerning, when applicable, data protection impact assessment and prior consultation with the supervisory authority, notification of a Personal Data Breach to the supervisory authority, communication of a Personal Data Breach to the Data Subject and responding to individuals exercising their rights under the applicable Data Protection Laws. The same obligations shall apply to any question, complaint or communication received by FORM.com from any data protection regulator or authority or other organization tasked with enforcing Data Protection Laws relating to FORM.com's provision of Services to Customer. To the extent legally permitted, Customer shall be responsible for any costs arising from FORM.com's provision of assistance herein.

4. SUB-PROCESSORS.

- a. Appointment of Sub-Processors. Customer agrees that FORM.com may engage FORM.com's Affiliates and third party Sub-Processors to Process Personal Data in connection with the provision of the Services. FORM.com has entered into a written agreement with each Sub-Processor containing data protection obligations not less protective than those in the Agreement with respect to the protection of Customer Data to the extent applicable to the nature of the Services provided by such Sub-Processor.
- b. List of Current Sub-Processors and Notification of New Sub-Processors. FORM.com has currently appointed, and Customer is giving its general authorization to use, as Sub-Processors, the FORM.com Affiliates and third-party Sub-Processors listed in Schedule 4 to this DPA. To receive

email notifications of any such updates, Customer may opt-in by subscribing to the additional or changed Sub-Processors list by sending a corresponding message to support@worldapp.com. FORM.com may also directly notify Customer in the event that additional or changed Sub-Processors are required to Process Customer Data in connection with the specific Services provided to Customer.

- c. **Objection Right.** Customer shall have a right to object to FORM.com's use of a new Sub-Processor by sending a written notice stating reasonable grounds for the objection to FORM.com within thirty (30) days after receiving a notice from FORM.com about a new Sub-Processor as described above. In the event Customer objects to a new Sub-Processor, as permitted in the preceding sentence, FORM.com will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected new Sub-Processor. FORM.com and Customer shall diligently work together to resolve any issues regarding objection to a new Sub-Processor provided by Customer. If FORM.com and Customer cannot resolve an objection issue within a reasonable period of time, FORM.com, in its sole discretion, shall either not appoint the objected-to new-Sub-Processor, or shall permit Customer to terminate the Agreement with respect only to those Services which cannot be provided by FORM.com without the use of the objected-to new Sub-Processor by sending a notice to FORM.com and without imposing a penalty on Customer for such termination. In the event the Agreement is terminated as noted, FORM.com will refund Customer fees pre-paid by Customer with respect to the terminated Services following the effective date of termination.
- d. **Liability.** FORM.com will remain responsible for each Sub-Processor's compliance with the obligations of this DPA and for any acts or omissions of such Sub-Processor that cause FORM.com to breach any of its obligations under this DPA.

5. DATA SUBJECT REQUEST.

To the extent that Customer is unable to independently address a Data Subject Request through the controls provided by the Services, then upon Customer's written request FORM.com will provide reasonable assistance to Customer to respond to any Data Subject Requests or requests from data protection authorities relating to the Processing of Personal Data under the Agreement. If a Data Subject Request or other communication regarding Processing of Personal Data is made directly to FORM.com, FORM.com will notify Customer without undue delay and will advise the Data Subject to

submit the request to Customer. Customer will be solely responsible for responding substantively to any such Data Subject Requests or communications involving Personal Data. Upon request by Customer, FORM.com may provide assistance to Customer in relation to any such Data Subject Request or communication involving Personal Data. The same obligations shall apply to any question, complaint or communication received by FORM.com from any data protection regulator or authority or other organization tasked with enforcing Data Protection Laws relating to FORM.com's provision of Services to Customer. To the extent legally permitted, Customer shall be responsible for any costs arising from FORM.com's provision of assistance herein.

6. LIMITATION OF LIABILITY.

Each party and each of their Affiliates' liability, taken in aggregate, arising out of or related to this DPA (and any other DPAs between the parties) and the Standard Contractual Clauses (where applicable), whether in contract, tort or under any other theory of liability, will be subject to the limitations and exclusions of liability set out in the Agreement. Any reference in such sections to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Agreement (including this DPA).

7. ADDITIONAL PROVISIONS FOR PROCESSING OF EUROPEAN PERSONAL DATA.

- a. GDPR. FORM.com will Process Personal Data in accordance with the GDPR requirements directly applicable to FORM.com's provision of Services.
- b. Roles of the Parties. The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Controller, FORM.com is the Processor and that FORM.com will engage Sub-Processors pursuant to the requirements set forth in Section 4 above.
- c. Details of Processing. The subject-matter of Processing of Personal Data by FORM.com is the performance of Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and categories of Data Subjects under this DPA are further detailed in Schedule 1 (Details of Processing) to this DPA.
- d. Transfer Mechanisms.
- e. FORM.com makes available the Standard Contractual Clauses set forth in Schedule 3 to this DPA which shall apply to any transfers of Personal Data under this DPA from the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom to

countries which do not ensure an adequate level of data protection within the meaning of Data Protection Laws and Regulations of the foregoing territories, to the extent such transfers are subject to such Data Protection Laws.

8. ADDITIONAL PROVISIONS FOR CALIFORNIA PERSONAL INFORMATION.

- a. CCPA. This section 8 of the DPA will apply only with respect to California Personal Information.
- b. Roles of the Parties. When Processing California Personal Information in accordance with the Instructions, the parties acknowledge and agree that Customer is a Business and FORM.com is a Service Provider for the purposes of the CCPA.
- c. Responsibilities. The parties agree that FORM.com will Process California Personal Information as a Service Provider strictly for the purpose of performing the Services under the Agreement (the "Business Purpose") or as otherwise permitted by the CCPA.

9. GOVERNING LAW.

This DPA shall be governed by and construed in accordance with governing law and jurisdiction provisions in the Agreement, unless required otherwise by Data Protection Laws.

List of Schedules

Schedule 1 – Details of Processing

Schedule 2 – Security Measures

Schedule 3 – Standard Contractual Clauses

Schedule 4 – List of Sub-Processors



The parties' authorized signatories have duly executed the DPA.

WORLDAPP, INC., by and on behalf of its affiliates, as applicable

Signature: DocuSigned by:
Ali Moosani
F60401F85500439...

Print Name: Ali Moosani

Title: CEO

Date: 12/10/2020

CUSTOMER, by and on behalf of its affiliates, as applicable

Signature: _____

Customer Legal Name: _____

Print Name: _____

Title: _____

Date: _____

SCHEDULE 1 – DETAILS OF PROCESSING

Nature and Purpose of Processing

FORM.com will Process Personal Data as necessary to perform the Services pursuant to the Agreement, as further specified in the Related Materials, and as further instructed by Customer in its use of the Services.

Duration of Processing

Unless otherwise set forth in the DPA, FORM.com will Process Personal Data for the duration of the Agreement, in accordance with the data storage procedures and timeframes set out in the Agreement.

Categories of Data Subjects

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Prospects, customers, business partners and vendors of Customer (who are natural persons)
- Employees or contact persons of Customer's prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of Customer (who are natural persons)
- Customer's Authorized Users

Type of Personal Data

Customer may submit Personal Data to the Services, the extent of which is determined and controlled by Customer in its sole discretion, and which may include, but is not limited to the following categories of Personal Data:

- First and last name
- Title
- Position
- Contact information (including company, email, phone, address)
- Any other Personal Data submitted by, sent to, or received by Customer, Authorized Users, or Customer's end users, through the Services.

Special categories of data (if appropriate)

FORM.com handles Customer Data provided by or through Customer. The parties do not anticipate the transfer of special categories of data unless expressly agreed by the parties.

Processing operations

Personal Data will be Processed in accordance with the Agreement (including this DPA) and may be subject to the following Processing activities:

- Storage and other Processing necessary to provide, maintain and improve the Services provided to Customer;
- To provide customer and technical support to Customer; and
- Disclosures as required by applicable laws or otherwise set forth in the Agreement.

SCHEDULE 2 – SECURITY MEASURES

Physical access controls

- Employed for preventing unauthorized persons from gaining access to Data Center processing systems within which Personal Data is processed or used.
- Electronic access card reading system
- Management of keys / documentation of key holders
- False entrances
- Vehicle blockades
- Customized parking lot designs
- Bulletproof glass/walls and unmarked buildings 24x7x365 staffed security guards
- Security service, front desk with required sign in for all visitors
- Burglar alarm system
- Internal and external infrared pan, tilt, zoom CCTV Monitored building management system
- Biometric scanners
- Portals and person-traps that authenticate only one person at a time
- Physical keys to locked cages containing the servers

Admission controls

- Measures taken for preventing data processing systems from being used without authorization.
- Personal and individual user log-in when entering the system and / or the corporate network
- Administrative accounts passwords requirements:
 - must contain at least 8 characters
 - must contain a mix of alpha and numeric characters
 - must be changed every 90 days
 - the history of the last 3 passwords is kept to ensure that the new password does not repeat one of the previous 3 passwords.
 - user accounts will be suspended for 5 minutes after 5 unsuccessful log-in attempts.
- Password procedures for standard users minimum of 8 characters, with a mix of alpha and numeric symbols.
- Application session times out after 40 minutes of inactivity

- Upon verification of the username and password, the application uses session-based token authentication.
- Remote access for maintenance requires IP-restricted remote access (SSH).
- Automated screen locks after 10 minutes of inactivity.
- Password protected screen savers.

Virtual access controls

- Measures taken to ensure that persons entitled to use a data processing system have access only to Personal Data to which they have a right of access, and that Personal Data cannot be read, copied, modified or removed without authorizations in the course of processing or use and after storage.
- User authentication is based on username and strong password
- All transactional records contain identifiers to distinguish Pilkington records.
- System processing uses a rule-based mechanism to tailor data access to specific users and roles.
- Data access, insert, and modification are logged.
- ISO certifications are maintained at the datacenter

Transmission controls

- Measures taken to ensure that Personal Data cannot be read, copied, modified or removed without authorization during electronic transmission or transport, and that it is possible to check and establish to which bodies the transfer of Personal Data by means of data transmission facilities is envisaged.
- All data are encrypted in flight using TLS
- Access to reports is logged
- Removable storage is not used

Input controls

- Measures taken to ensure that it is possible to check and establish whether and by whom Personal Data have been entered into data processing systems, modified or removed.
- Application provides an option to restrict record entry to a defined set of roles.
- Application provides an option to date/time stamp the entries and include identifiers for entering party.

- Firewalls and intrusion prevention systems are in place to prevent unauthorized access

Assignment controls

- Measures employed to ensure that, in the case of commissioned Processing of Personal Data, the data are processed strictly in accordance with the instructions of the principal.
- Confidentiality agreements are in place for all individuals with data access
- Training is conducted during onboarding and on a regular basis
- No third parties used for the processing of data other than as described in this Agreement.
- Privacy policy describes rights and obligations of agent and principle

Availability controls

- Measures taken to ensure that Personal Data are protected from accidental destruction or loss.
- Systems employ redundancies such as RAID arrays and redundant equipment.
- Backups are stored in alternate equipment from primary processing.
- Multiple air conditioning units are installed to provide redundant capacity in a N+1 configuration.
- Fire protection including "sniffer" systems, augmented by heat detection and dry-pipe sprinkler systems.
- Multiple firewall layers and hardening on all servers.
- UPS backed by N+1 generators.
- Diverse fiber routing and multiple carriers.

Separation controls

- Measures taken to ensure that Personal Data collected for different purposes can be processed separately.
- Three-tier systems are used to physically separate presentation, business processing and storage.
- Separation of duties is used internally to ensure functions pass through change control processes.
- Discrete development, staging and production environments are maintained.
- All routing of data for processing is controlled through automated rules engines.
- Computing and storage is on equipment owned by Processor.

SCHEDULE 3 – STANDARD CONTRACTUAL CLAUSES

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection,

The Customer, as defined in Schedule 1 of the DPA (the “data exporter”)

And

WorldAPP, Inc., 222 Forbes Road, Suite 303, Braintree, MA 02184 (the “data importer”)

each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

‘personal data’, ‘special categories of data’, ‘process/processing’, ‘controller’, ‘processor’, ‘data subject’ and **‘supervisory authority’** shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

‘the data exporter’ means the controller who transfers the personal data;

‘the data importer’ means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country’s system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

‘the subprocessor’ means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on

behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

'technical and organisational security measures' means those measures aimed at protecting personal 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.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any

successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

1. Obligations of the data exporter

The data exporter agrees and warrants:

- (a.) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- (b.) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- (c.) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
- (d.) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal 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;
- (e.) that it will ensure compliance with the security measures;
- (f.) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

- (g.) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- (h.) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- (i.) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
- (j.) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

- (a.) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (b.) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (c.) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
- (d.) that it will promptly notify the data exporter about:

- (e.) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;
- (f.) any accidental or unauthorised access; and
- (g.) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- (h.) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- (i.) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
- (j.) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
- (k.) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
- (l.) that the processing services by the subprocessor will be carried out in accordance with Clause 11;
- (m.) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any

of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
 - (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
 - (b) to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9

Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes

the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data-processing services

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.



On behalf of the data exporter:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

(stamp of organization)

Signature: _____

On behalf of the data importer:

Name (written out in full): Ali Moosani

Position: CEO

Address: 222 Forbes Road, Suite 303, Braintree, MA 02184

Other information necessary in order for the contract to be binding (if any):

(stamp of organization)

Signature: _____  F60401F85500439...



APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Standard Contractual Clauses (the 'Clauses').

Data exporter

The data exporter is the legal entity specified as "Customer" in the DPA.

Data importer

The data importer is WorldAPP, Inc. or Designlogic Ltd.

Data subjects

Please see Schedule 1 of the DPA, which describes the data subjects.

Categories of data

Please see Schedule 1 of the DPA, which describes the categories of data.

Special categories of data (if appropriate)

Please see Schedule 1 of the DPA, which describes the special categories of data.

Processing operations

The objective of Processing Personal by data importer is the performance of the Services pursuant to the Agreement.

Please see Schedule 1 of the DPA, which describes the processing operations.

DATA EXPORTER

Name: _____

Authorized Signature: _____

DATA IMPORTER

Name: Ali Moosani _____
DocuSigned by:

Authorized Signature: Ali Moosani _____
F60401F85500439...



APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Standard Contractual Clauses (the 'Clauses').

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Please see Schedule 2 of the DPA, which describes the security measures by FORM.com.

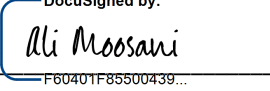
DATA EXPORTER

Name: _____

Authorized Signature: _____

DATA IMPORTER

Name: Ali Moosani _____

Authorized Signature: _____

F60401F85500439...

SCHEDULE 4 – LIST OF SUB-PROCESSORS

The list below the Sub-Processors that are currently relied upon by FORM.com in connection with the Services and may be used in connection with FORM.com’s Processing of Customer Data.

Entity Name	Subprocessing Activities	Country
Microsoft Corporation (e.g., Azure, O365)	Information Technology Support Services	United States
Salesforce.com, Inc.	Internal Operations Support Services	United States
Hubspot, Inc.	Internal Operations Support Services	United States
ZenDesk, Inc.	Internal Operations Support Services	United States
Qlik Technologies, Inc.	Optional Reporting Capability	United States
Lumen Technologies (Century Link)	Cloud Hosting Infrastructure	United States
Amazon Web Services, Inc.	Cloud Hosting Infrastructure	United States

This list may be updated from time to time as Sub-Processors are added or removed. To receive email notifications of any such updates, Customer may opt-in by subscribing to the additional or changed Sub-Processors list by sending a corresponding message to support@worldapp.com. FORM.com may also directly notify Customer in the event that additional or changed Sub-Processors are required to Process Customer Data in connection with the specific Services provided to Customer.