



# DATA PROCESSING AGREEMENT

**Revision Date: January 3, 2024**

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. and/or its Affiliates (hereinafter referred together as “FORM”) 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), and all amendments thereto including, but not limited to CPRA.

“**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’ use 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 but not limited to the California Consumer Privacy Act, Virginia Consumer Data Protection Act, Utah Consumer Privacy Act, Colorado Privacy Act, Connecticut Data Privacy Act), 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.

**“Public Authority Access”** means either a request for disclosure of Personal Data or direct access to Personal Data by a public authority.

**“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, 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 and/or FORM’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 pursuant to the terms of an applicable Agreement.

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

**“Third Party Request”** means a written request from a third party for disclosure of (or access to) Personal Data, including a Public Authority Access request, where compliance with such request is required by Applicable Law.

**“FORM”** means WorldAPP, Inc. and/ or its Affiliates, including, without limitation, 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. 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 FORM for Processing in accordance with the terms of the Agreement and this DPA, and ensuring the Customer's Instructions to FORM 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 in relation to the Processing of Personal Data, and additional instructions outside the scope of the Instructions shall require prior written agreement between FORM and Customer. Form shall inform Customer if, in its opinion, a processing instruction infringes applicable legislation and/or regulation.
- c) **Data Transfers.** Customer acknowledges and agrees that FORM 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 in the United States and to other jurisdictions where FORM Affiliates and third-party Sub-Processors have operations. FORM shall comply with the reasonable requirements for transfer of Personal Data to third countries which are set out by applicable laws, if any.

## 3. FORM OBLIGATIONS.

- a) **Limitation of Access.** FORM will ensure that FORM'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 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, 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. FORM is not responsible for compliance with any Data Protection Laws applicable to Customer or Customer's industry that are not generally applicable to FORM.
- c) **Compliance with Instructions.** FORM 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 will make available to Customer all information reasonably necessary to demonstrate compliance with this DPA and allow for audits in order to assess compliance with this DPA, 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 will ensure that any personnel engaged by FORM in the Processing of Personal Data are subject to appropriate confidentiality obligations (whether a contractual or statutory obligation).
- f) **Security.** FORM 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 will regularly monitor compliance with such Security Measures. FORM 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 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 will make reasonable efforts to identify the cause of such Personal Data Breach and take those steps as FORM deems necessary and reasonable to remediate the cause of such Personal Data Breach to the extent the remediation is within FORM’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 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 is required by applicable law or contract to retain any Customer Data, or to Customer Data archived on back-up systems as described in the Agreement.
- i) **Other Assistance.** FORM, 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 from any data protection regulator or authority, or other organization tasked with enforcing Data Protection Laws relating to FORM’s provision of Services to Customer. To the extent legally permitted, Customer shall be responsible for any costs arising from FORM’s provision of assistance herein.

## 4. SUB-PROCESSORS.

- a) **Appointment of Sub-Processors.** Customer agrees that FORM may engage FORM’s Affiliates and third-party Sub-Processors to Process Personal Data in connection with the provision of the Services. FORM has entered into a written agreement with each third-party 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 third-party Sub-Processor.

- b) **List of Current Third-Party Sub-Processors and Notification of New Third-Party Sub-Processors.** FORM has currently appointed, and Customer is giving its general authorization to use, as Sub-Processors, FORM Affiliates, whether or not they are indicated herein, and third-party Sub-Processors listed in Schedule 3 to this DPA. To receive email notifications of any updates to the third-party Sub-Processors list, Customer may opt-in by subscribing to the additional or changed third-party Sub-Processors list by sending a corresponding message to support@worldapp.com or, where Customer doesn't want to opt-in by subscribing, to monitor the current third-party Sub-Processors list available in the current version of this DPA published on FORM's website. FORM 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's use of a new third-party Sub-Processor by sending a written notice stating reasonable grounds for the objection to FORM within thirty (30) days after receiving a notice from FORM about a new third-party Sub-Processor or, where Customer doesn't want to opt-in by subscribing to the additional or changed third-party Sub-Processors list, within thirty (30) days after publishing of the renewed third-party Sub-Processors list on FORM's website as described above. In the event Customer objects to a new Sub-Processor, as permitted in the preceding sentence, FORM 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 and Customer shall diligently work together to resolve any issues regarding objection to a new Sub-Processor provided by Customer. If FORM and Customer cannot resolve an objection issue within a reasonable period of time, FORM, 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 without the use of the objected-to new Sub-Processor by sending a notice to FORM and without imposing a penalty on Customer for such termination. In the event the Agreement is terminated as noted, FORM will refund Customer fees pre-paid by Customer with respect to the terminated Services following the effective date of termination.
- d) **Liability.** FORM 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 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 will provide reasonable assistance to Customer by appropriate technical and organizational measures, insofar as this is possible, 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, FORM





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 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 from any data protection regulator or authority, or other organization tasked with enforcing Data Protection Laws relating to FORM's provision of Services to Customer. To the extent legally permitted, Customer shall be responsible for any costs arising from FORM's provision of assistance herein.

## 6. THIRD-PARTY REQUEST.

Where FORM receives a Third-Party Request or becomes aware of Public Authority Access in relation to Personal Data transferred to it, FORM shall promptly notify Customer, if permitted under the applicable law, and provide all information available to it including, but not limited, the requesting party, legal grounds for the request and a response provided to the third party, if any.

If FORM is prohibited from notifying Customer of a Third-Party Request or Public Authority Access, it shall use its best efforts to obtain a waiver of the prohibition to notify Customer.

FORM acknowledges and agrees that it shall evaluate the Public Authority Access as to the legality of the Personal Data disclosure. If, after a thorough analysis, FORM concludes that under the law there are grounds for challenging the request, it shall exhaust all remedies to challenge the request received. FORM shall take commercially reasonable measures to suspend the effects of the request until the court has decided on the merits.

FORM shall document its assessment and challenge of the request for disclosure and notify the competent supervisory authority from the European Economic Area about the received request, insofar as possible under the law or request.

FORM shall only provide the minimum amount of information possible, based on a reasonable interpretation of the request.

To the extent legally permitted, Customer shall be responsible for any costs arising from FORM's provision of assistance herein.

## 7. 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).

## 8. ADDITIONAL PROVISIONS FOR PROCESSING OF EUROPEAN PERSONAL DATA.

- a. **GDPR.** FORM will Process Personal Data in accordance with the GDPR requirements directly applicable to FORM'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 is the Processor, and that FORM 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 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.**

FORM (the US companies and affiliates) complies with EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S. DPF as set forth by the U.S. Department of Commerce. FORM has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union in reliance on the EU-U.S. DPF and from the United Kingdom (and Gibraltar) in reliance on the UK Extension to the EU-U.S. DPF. Thus, in its data transfers from the EU and UK to US FORM relies on the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the DPF as an adequate means of protection of the personal data.

Customer and FORM acknowledge and agree that to the extent that the data protection legislation of Switzerland applies to the data transfers by the data exporter, the Standard Contractual Clauses (Controller to Processor) are incorporated herein by reference and are an integral part of this DPA. Customer shall be the data exporter and FORM shall be the data importer for the purposes of the Standard Contractual Clauses. The following changes to the Standard Contractual Clauses shall apply for the enforcement and operation of the Standard Contractual Clauses for transfers made by the Swiss data exporter to the data importer:

1. in Clause 7, the optional docking clause will not apply;
2. in Clause 9, Option 2 will apply, and the time period for prior notice of Sub-processor changes shall be as set out in Section 4 of this DPA;
3. in Clause 11, the optional language will not apply;
4. in Clause 17, Option 1 will apply, and the EU SCCs will be governed by the Swiss law;
5. in Clause 18(b), disputes shall be resolved before the courts of Switzerland;
6. Annex I of the EU SCCs shall be deemed completed with the information set out in Schedule 1 to this DPA; and
7. Annex II of the EU SCCs shall be deemed completed with the information set out in Schedule 2 to this DPA.



8. References to the 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) or specific articles of the Regulation shall be replaced with reference to the Swiss data protection laws and applicable articles therein;
9. References to the Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC shall be deleted;
10. Any references to the EU, European Union, Union, Member State shall be replaced with references to Switzerland accordingly.
11. Data transfers governed by Swiss data protection legislation are also covered by the Standard Contractual Clauses in case of the transfer of information relating to an identified or identifiable legal entity where such information is protected similarly as Personal Data under Swiss data protection legislation until such laws are amended to no longer apply to a legal entity.

## 9. ADDITIONAL PROVISIONS FOR PROCESSING OF CALIFORNIA PERSONAL INFORMATION.

- a. **CCPA.** This section 9 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 is a Service Provider for the purposes of the CCPA.
- c. **Responsibilities.** The parties agree that FORM 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.

## 10. GOVERNING LAW.

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

### List of Schedules

Schedule 1 – Details of Processing

Schedule 2 – Security Measures

Schedule 3 – List of Third-Party Sub-Processors

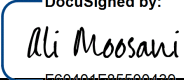




The parties' authorized signatories have duly executed the DPA.

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

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

DocuSigned by:  
  
 Signature: \_\_\_\_\_  
 Print Name: Ali Moosani  
 Title: CEO  
 Date: 1/3/2024

Signature: \_\_\_\_\_  
 Customer Legal Name: \_\_\_\_\_  
 Print Name: \_\_\_\_\_  
 Title: \_\_\_\_\_  
 Date: \_\_\_\_\_





# SCHEDULE 1 – DETAILS OF PROCESSING

## Nature and Purpose of Processing

FORM 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 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 or contact persons of Customer (who are natural persons)  
Customer's Authorized Users or end 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 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.

## Purpose(s) of the data transfer and further processing:

Performance of the services under the service agreement.

## Other applicable information:

**The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:**

Data importer will process personal data for the duration of the agreement, in accordance with the data storage procedures and timeframes set out in the service agreement.

**The frequency of the transfer** continuous basis.

**Data importer's representative in the European Union:** DPO Consulting, in Paris, France.

**Data importer's representative in the European Union email address:** [dpo\\_eu@form.com](mailto:dpo_eu@form.com)

**Data importer's representative in the UK:** Designlogic Limited, Hampshire, UK

**Data Importer's Data Protection Officer's email contacts:** [dpo@form.com](mailto:dpo@form.com) or (781) 849-8118.

**For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:**

Personal data may be transferred to (sub-) processors for performance of services, as further instructed by data importer in its use of the services. (Sub-) processors will process personal data for the duration of the service agreement, in accordance with the data storage procedures and timeframes set out in the service agreement. List of the Sub-processors used for the provision of the Services and their country of location is attached as a Schedule 3 to the DPA.



## SCHEDULE 2 – SECURITY MEASURES

FORM is ISO27001 and 27701 certified.

The following technical and organizational measures are performed on the processes taken by FORM:

### 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 make sure 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 a 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 – LIST OF THIRD-PARTY SUB-PROCESSORS

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

Entity Name	Description of Sub-Processing Activities	Location
<b>Microsoft Corporation (e.g., Azure, O365)</b>	Information Technology Support Services	Microsoft Corporation, One Microsoft Way, Redmond, Washington 98052-6399, United States
<b>Salesforce.com, Inc.</b>	Internal Operations Support Services	Salesforce.com, Inc. Salesforce Tower, 415 Mission Street, 3rd Floor, San Francisco, CA 94105, United States
<b>ZenDesk, Inc.</b>	Internal Operations Support Services	989 Market St, San Francisco, CA 94103, United States
<b>Lumen Technologies (Century Link)</b>	Hosting Infrastructure	100 Centurylink Dr, Monroe, LA 71203, United States
<b>Warrior Developers</b>	Operations Services	1100 Glendon Ave., Suite 920 Los Angeles, California 90024
<b>Atlassian</b>	Jira	Atlassian Pty Ltd c/o Atlassian, Inc. 350 Bush Street, Floor 13 San Francisco, CA 94104 E-Mail: <a href="mailto:privacy@atlassian.com">privacy@atlassian.com</a>
<b>Gearset</b>	Salesforce backups	Gearset Limited, The Bradfield Centre, Cambridge Science Park Rd, Cambridge, CB4 0GA, UK
<b>Google Cloud (Google Inc.)</b>	Hosting Infrastructure	1600 Amphitheatre Parkway Mountain View, CA 94043, USA <a href="tel:6502530000">(650) 253-0000</a>
<b>FORM Affiliates</b>		
<b>GSC Helium, LLC</b>	In-house Operations	859 Willard Street, Suite 400, Quincy MA 02169 United States





<b>Designlogic Limited</b>	In-house Operations	The Square, Basing View, Basingstoke, Hampshire, RG21 4EB UK
<b>ShelfWise Sp. z o.o.</b>	In-house Operations	ul. Berka Joselewicza 21C 31-031 Kraków Poland <a href="mailto:hello@shelfwise.ai">hello@shelfwise.ai</a>

This list may be updated from time to time as third-party 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](mailto:support@worldapp.com) or, where Customer doesn't want to opt-in by subscribing, to monitor the current third-party Sub-Processors list available in the current version of this DPA published on FORM's website. FORM 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.

