MASTER SERVICES AGREEMENT

TERMS AND CONDITIONS

This Master Service Agreement ("Agreement") shall apply to the sale of Services from Convercent, Inc. ("Convercent") to its customer ("Customer"), unless Convercent and Customer enter into or have entered into another agreement regarding the Services contemplated herein, and such agreement is in effect as of the Effective Date ("Existing Agreement"), in which case the terms and conditions of the Existing Agreement shall govern the sale of those Convercent Services. Absent an Existing Agreement, this Agreement is effective as of the date an Order Form or Purchase Order is executed ("Effective Date").

1. SERVICES.

1.1 **Use of the Services**. Customer may use the Services ordered by Customer solely for Customer's internal business purposes. Customer may grant administrative access and authority in relation to the Services to employees or contractors of Customer's organization ("**Administrative Users**"), provided that Customer will remain responsible and liable for all actions or omissions of its Administrative Users in connection with the Services. Customer may purchase implementation and configuration Services from Convercent but notwithstanding any such Services, Customer will be solely responsible for; (a) configuring or determining how the Services will be configured for Customer's use; (b) providing for and maintaining any systems, software, hardware, web browser and internet service necessary to access and use the Services; (c) establishing, managing, maintaining, and supporting access rules, incident reporting protocols, authorization of Customer representatives to receive incident reports and communications and any other distribution rules regarding the Services or information contained therein, and (d) providing legally required and appropriate disclosures, and the content thereof, to third parties making reports through the Services. Customer may submit written incident reports online through the Services in English or in another supported language indicated within the Services.

1.2 **Restrictions**. Customer will not (a) modify, make derivative works of, reverse engineer, disassemble, decompile, or otherwise attempt to discover the source code for the Services; (b) use, evaluate or view the Services for the purpose of designing, modifying, or otherwise creating any environment, program, or infrastructure or any portion thereof, which performs functions similar to the functions performed by the Services; or (c) remove or alter any trademark, logo, copyright, or other proprietary notices, legends, symbols, or labels in the Services.

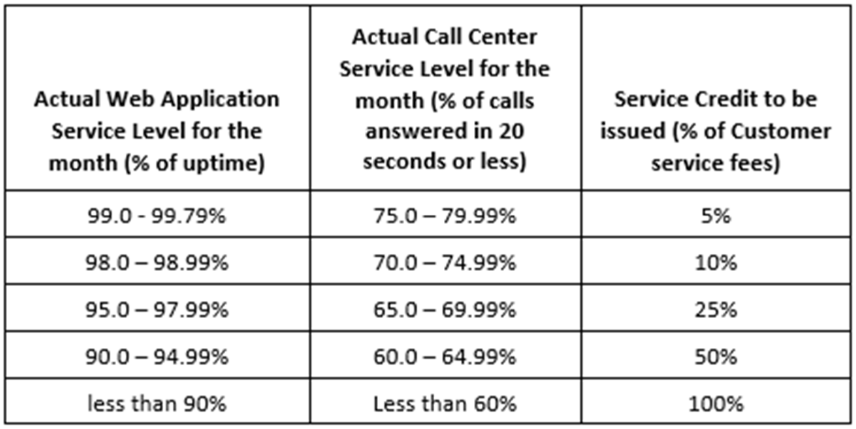
1.3 **Employee Count**. Services sold on a subscription-fee basis are priced according to the total number of employees and individual independent contractors of Customer ("**Employee Count**"). Customer represents the initial Employee Count specified on each Order Form is accurate. Additionally, Convercent may request no more than once annually an updated Employee Count from Customer. For any increase in the Employee Count greater than five percent (5%), Convercent reserves the right to adjust the pricing ratably for all subscription-fee based Services purchased by Customer hereunder.

1.4 **Service Levels**.

a. *Web Application*. Convercent will maintain 99.8% uptime of the web-based Services (the "**Web Application SLA**"). The calculation of uptime will exclude scheduled downtime and Force Majeure Events (as defined below). Convercent will inform Customer at least forty-eight (48) hours in advance of any scheduled downtime.

b. *Call Center*. The call center will be available to receive telephonic reports in the event of an outage within the web application and 80% of calls to the call center will be answered in 20 seconds or less (the "**Call Center SLA**", which, together with the Web Application SLA, the "**SLAs**").

c. *Remedy*. Convercent's sole liability (and Customer's exclusive remedy) for Convercent's breach of either or both SLAs will be to issue a service credit ("**Service Credit**") for the applicable Services for the applicable month, in the amount specified in the table below, which Customer must request by emailing AP@convercent.com within thirty (30) days following the end of the month in which the service level failure occurred. In the event two SLA remedies apply, only the Service Credit for the higher amount will apply. Customer may review the Convercent Community for the performance of the SLAs.



Actual Web Application Service Level for the month (% of uptime)	Actual Call Center Service Level for the month (% of calls answered in 20 seconds or less)	Service Credit to be issued (% of Customer service fees)
99.0 - 99.79%	75.0 – 79.99%	5%
98.0 – 98.99%	70.0 – 74.99%	10%
95.0 – 97.99%	65.0 – 69.99%	25%
90.0 – 94.99%	60.0 – 64.99%	50%
less than 90%	Less than 60%	100%

1.5 **Professional Services**. Any professional or advisory Services ordered by Customer hereunder will be provided in accordance with industry standard practices. Any such Services will not constitute legal advice and Customer's use of the Services will not create an attorney client relationship between Customer and Convercent. Customer will not request any legal advice as part of the Services and will consult with independent counsel regarding Customer's use and configuration of the Services.

2. INTELLECTUAL PROPERTY.

2.1 **The Services**. The Services are licensed, not sold. Convercent and its suppliers exclusively own and retain all rights, title, and interest in and to the Services (including software, user interface designs, and documentation) and all additions and modifications to the Services, including all intellectual property rights therein.

2.2 **Customer Data**. "**Customer Data**" means all data (including Personal Data as defined below), information, reports, policies, and other content imported to the Services or otherwise provided to Convercent or its contractors by or for Customer in connection with Customer's use of the Services, and all data and information received by or for Customer from Customer's use of the Services. Customer exclusively owns and retains all rights, title, and interest in and to the Customer Data, except for pre-existing Services components contained in such Customer Data (e.g., incident report templates). Customer hereby grants to Convercent and its authorized representatives and contractors a non-exclusive and non-transferable right and license to use, process, store, and transmit, and disclose Customer Data solely to provide the Services to Customer and fulfill other obligations described in this Agreement. Customer further authorizes Convercent to anonymize Customer Data and to aggregate Customer Data with similar data from other Convercent customers in a manner that does not identify Customer or include any Personal Data, to further develop and provide services for Convercent customers.

2.3 **Customer Name and Logo Use**. During the Term, Convercent may include Customer's name and logo in Convercent's standard marketing materials, customer lists, name Customer in proof points, case studies, and customer stories, provided that Convercent will first obtain Customer's consent for any such use.

3. FEES AND TAXES.

3.1 **Fees**. The fees for all Services will be set forth in each Order Form ("**Fees**") and Customer will pay all such Fees in accordance with the terms of this Agreement and the applicable Order Form. Unless otherwise set forth in the applicable Order Form, all Fees due hereunder will be paid annually in advance in U.S. dollars, and will be due within 30 days of the date of the invoice therefor. Should Customer require a PO to purchase, such PO must be issued within 10 days of the Order Effective Date (as defined in the Order Form).

3.2 **Taxes**. Convercent's fees do not include any taxes, levies, duties, or similar governmental assessments of any nature (collectively, "**Taxes**"). Customer is responsible for paying all Taxes associated with its purchases hereunder, excluding taxes on Convercent's net income. If Convercent has the legal obligation to pay or collect Taxes for which Customer is responsible under this Agreement, Convercent will invoice Customer and Customer will pay that amount unless Customer provides Convercent a valid tax exemption certificate from the appropriate taxing authority.

4. TERM AND TERMINATION.

4.1 **Term**. This Agreement will commence on the Effective Date and, unless earlier terminated in accordance with the Termination for Cause Section, below, will remain in effect so long as any Order Form remains in effect or any services are provided hereunder (collectively, the "**Term**").

4.2 **Suspension.** At any time during the Term, Convercent may, immediately upon notice to Customer, suspend access to any Service in the event of a threat to the technical security or technical integrity of the Services.

4.3 **Termination for Cause**. Either party may terminate this Agreement upon written notice if the other party is in material breach of this Agreement and such breach remains uncured for thirty (30) days following the breaching party's receipt of written notice of such breach.

4.4 **Effect of Termination**. Upon expiration or termination of this Agreement for any reason: (a) the rights and licenses granted hereunder will cease and the Services will immediately terminate, (b) if requested by Customer, Convercent will, at Customer's cost, make available to Customer (via an SFTP site, for example) the Customer Data held by Convercent (and Customer will assume responsibility for its copy of such Customer Data (and any access thereto) upon download of the Customer Data), and (c) if requested by Customer, Convercent will take reasonable steps to assist with transfer of any dedicated phone numbers used by Convercent or its contractors in connection with the Service. Upon termination by Customer for Convercent's breach, prepaid Fees for Services applicable to the period following termination will be refunded to Customer, less any unpaid Fees for Services. Termination of the Agreement will be without prejudice to either party's rights to seek recovery of damages or pursue any other remedies it may have hereunder or under applicable law. The Restrictions, Intellectual Property, Fees and Taxes, and Effect of Termination Sections, as well as all Sections from and including

Confidentiality through General Provisions, will survive the expiration or termination of this Agreement for any reason.

5. CONFIDENTIALITY. Each party acknowledges that the Confidential Information (as hereinafter defined) of the other party may contain information valuable to the Disclosing Party, and each party that receives such Confidential Information (the "**Receiving Party**") from the other party (the "**Disclosing Party**") agrees that Confidential Information will remain the property of the Disclosing Party. Receiving Party will not make use of Disclosing Party's Confidential Information, except as authorized by this Agreement and to the extent necessary for performance or enforcement of this Agreement; and Receiving Party will keep Disclosing Party's Confidential Information confidential and not disclose to any third party, except to such Receiving Party's employees and contractors who need to know such information in order for such party to perform this Agreement and only to the extent they are bound by confidentiality and non-use obligations not less restrictive than this Agreement. If Customer provides any general feedback, comments, or ideas to Convercent regarding the Services or improvements thereto that does not specifically relate to Customer Data or Customer Confidential Information, Customer agrees that Convercent will be free to use, disclose, and exercise any rights in the same in connection with its products and services. "**Confidential Information**" means all information that is, or should be reasonably understood to be, confidential or proprietary information of the Disclosing Party (and its suppliers, contractors and customers), including without limitation information concerning its business, products, services, finances, employees, contractors, software, notes, documentation, tools, processes, protocols, product designs and plans, customer lists and other marketing and technical information; and the terms of this Agreement, whether disclosed orally or in writing by any other media. Confidential Information includes all software and related user documentation included in the Services, Customer Data, and excludes information that (a) is or becomes generally known to the public through no fault or breach of this Agreement by the Receiving Party; (b) is independently developed by a party without reference to the Confidential Information of the other party; (c) was in the Receiving Party's possession free of any obligation of confidence at the time it was communicated to the Receiving Party; or (d) is rightfully obtained by a party from a third party without restriction on use or disclosure. Notwithstanding the foregoing, the Receiving Party will not be in violation of this Section with regard to disclosure of Confidential Information in response to an order or subpoena of a court, agency or tribunal of competent jurisdiction, or pursuant to any applicable law or regulation, provided that the Receiving Party provides the Disclosing Party with prior written notice of such disclosure to the extent reasonably practicable and legally permissible in order to permit the Disclosing Party to seek confidential treatment of such information.

6. REPRESENTATIONS AND WARRANTIES; DISCLAIMER.

6.1 Warranties. Each party represents and warrants to the other party that (a) it has and will have full right and authority to enter into this Agreement and to grant the rights provided hereunder, (b) this Agreement will be enforceable against it, and (c) the entry into and performance of this Agreement by it do not contravene other agreements, laws, or orders to which it is subject. Customer represents and warrants that Customer will not make or publish any representations, warranties, or guarantees about the performance of the Convercent Services to any users of the Services.

6.2 Disclaimer. EXCEPT AS EXPRESSLY PROVIDED IN THIS REPRESENTATIONS AND WARRANTIES; DISCLAIMER SECTION, NEITHER PARTY MAKES ANY REPRESENTATIONS OR WARRANTIES OF ANY KIND AND EACH PARTY SPECIFICALLY DISCLAIMS ALL OTHER REPRESENTATIONS, WARRANTIES, AND CONDITIONS, WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT AND ANY WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. WITHOUT LIMITING THE FOREGOING, CONVERCENT DOES NOT REPRESENT OR WARRANT THAT THE SERVICES WILL MEET ALL OF CUSTOMER'S REQUIREMENTS OR BE UNINTERRUPTED, SECURE, COMPLETE, ERROR-FREE, OR FREE OF VIRUSES, MALICIOUS CODE, OR OTHER HARMFUL COMPONENTS, OR THAT ALL DEFECTS WILL BE CORRECTED.

7. INDEMNIFICATION.

7.1 By Convercent. Convercent will indemnify, defend, and hold harmless Customer from and against any third-party suit and the damages finally awarded therein ("**Claim**") which alleges that the Services infringe, misappropriate or violate the intellectual property right of any third party.

7.2 By Customer. Customer will indemnify, defend, and hold harmless Convercent from and against any and all Claims which allege that any Customer Data infringes, misappropriates or violates the intellectual property right of any third party or relate to or are based on Customer's handling of or the content of incident reports successfully received by the Customer via the Services.

7.3 Indemnification Procedure. Each party's indemnification obligation above is subject in each instance to the indemnified party (a) promptly giving notice of the Claim to the indemnifying party; (b) giving the indemnifying party sole control of the defense and settlement of the Claim (provided that the indemnified party will have the right to approve any material liability imposed on and borne by the indemnified party in connection with such settlement); and (c) providing to the indemnifying party all available information and reasonable assistance.

7.4 Exceptions. Notwithstanding the foregoing, Convercent will not have any indemnification obligations pursuant to this Agreement to the extent any Claim arises from (a) use of the Services outside the scope of the rights granted to Customer in this Agreement; (b) use of the Services with other products, software or materials not furnished by Convercent where the Services would not themselves be infringing; or (c) the modification or improvement of the Services by Customer or any third party; or (d) any continued use by Customer of an allegedly infringing item or continued allegedly infringing activity by Customer after Convercent has replaced or modified the item or instructed Customer to modify the activity so that it becomes non-infringing.

7.5 Replacement or Modification. Should the use of any Services or portion thereof be enjoined or threatened to be enjoined or determined to be infringing any third party intellectual property right, Convercent will notify Customer and, at Convercent's expense Convercent may: (a) procure for Customer the right to continue use of the Services as contemplated under this Agreement, (b) replace or modify the Services to be non-infringing, or (c) if "(a)" or "(b)" are not economically feasible for Convercent, then Convercent will have the right to terminate the obligations with regards to such Services consistent with the Effect of Termination Section.

8. Limitation of Liability. EXCEPT FOR A PARTY'S BREACH OF THE CONFIDENTIALITY SECTION AND A PARTY'S OBLIGATIONS PROVIDED IN THE INDEMNIFICATION SECTION, NEITHER PARTY WILL BE LIABLE TO THE OTHER FOR ANY LOSS OF PROFITS, LOSS OF BUSINESS, FINES OR PENALTIES, COSTS OF PROCUREMENT OF SUBSTITUTE SERVICES OR TECHNOLOGY, LOSS OF USE OR DATA, INTERRUPTION OF BUSINESS, OR FOR INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES OF ANY KIND, REGARDLESS OF THE LEGAL OR EQUITABLE THEORY ON THE BASIS OF WHICH ANY CLAIM FOR DAMAGES IS BROUGHT, INCLUDING, BUT NOT LIMITED TO, BREACH OF CONTRACT, TORT OR STATUTE, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. EXCEPT FOR A PARTY'S BREACH OF THE CONFIDENTIALITY SECTION, (A) A PARTY'S OBLIGATIONS PROVIDED IN THE INDEMNIFICATION SECTION, AND CUSTOMER'S PAYMENT OBLIGATIONS UNDER THE APPLICABLE ORDER FORM, IN NO EVENT WILL EITHER PARTY'S AGGREGATE LIABILITY TO THE OTHER ARISING OUT OF OR RELATING TO THIS AGREEMENT EXCEED THE TOTAL FEES PAID BY CUSTOMER TO CONVERCENT UNDER THE APPLICABLE ORDER FORM DURING THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE EVENT FIRST GIVING RISE TO THE LIABILITY (THE "**GENERAL LIABILITY CAP**") AND (B) IN NO EVENT WILL CONVERCENT'S AGGREGATE LIABILITY TO CUSTOMER ARISING OUT OF OR RELATING TO ANY SECURITY BREACH OR ANY BREACH BY CONVERCENT OF THE DATA PROTECTION SECTION EXCEED THE LESSER OF TEN (10) TIMES THE GENERAL LIABILITY CAP OR ONE MILLION DOLLARS ($1,000,000).

9. **Compliance with Law**. In performing its obligations or exercising its rights under this Agreement, each party will comply with all applicable laws, rules, and regulations.

10. DATA PROTECTION.

10.1 **Personal Data**. In the course of performing the Services for Customer, Convercent may receive and store information included within Customer Data that can be used to uniquely identify, contact or locate a natural person, including but not limited to name, address, email address, or phone number ("**Personal Data**"). Convercent will safeguard the confidentiality of Personal Data in accordance with Exhibit A and will not access or use such Personal Data other than as necessary to perform the Services or as otherwise expressly permitted hereunder. Convercent receives and stores Personal Data solely as an agent acting on behalf of Customer.

10.2 **Security**. The Convercent product and applications are ISO 27001:2013, SOC 2, HITRUST CSF certified or an equivalent and Convercent will protect all Customer Data as described in Exhibit A. At Customer's request, no more than once per year, Convercent will provide to Customer third party assessments and compliance certifications it makes available to all customers, including an annual Service Organization Controls (SOC) 2 Type II report ("**SOC 2 Report**") as defined by the American Institute of Certified Public Accountants. Such SOC 2 Report will include an opinion by the independent auditor on the adequacy and integrity of Convercent's general controls for security.

10.3 **EU Law**. If the parties agree that the Services will involve the processing by Convercent of Personal Data from the European Union, then Convercent will perform all such processing in compliance with the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) and the Data Processing Addendum that the parties will attach hereto as Exhibit B.

11. GENERAL PROVISIONS.

11.1 **Independent Contractors**. The parties are independent contractors, and no agency, partnership, franchise, joint venture, or employment relationship is intended or created by this Agreement.

11.2 **Severability**. If any provision herein is held to be invalid or unenforceable for any reason, the remaining provisions will continue in full force and effect without being impaired or invalidated in any way. The parties agree to replace any invalid provision with a valid provision that most closely approximates the intent and economic effect of the invalid provision.

11.3 **Waiver**. Neither party will be deemed to have waived any provision hereof unless such waiver is in writing and executed by a duly authorized officer of both parties. Except as otherwise set forth in this Agreement, no failure to exercise or delay in exercising any rights arising from this Agreement will operate or be construed as a waiver thereof.

11.4 **Force Majeure**. With the exception of any monetary obligations under this Agreement, neither party will be responsible for performance of its obligations hereunder where delayed or hindered by events beyond its reasonable control, including, without limitation, acts of God or any governmental body, war or national emergency, riots or insurrection, pandemic or epidemic, sabotage, embargo, fire, flood, accident, strike or other labor disturbance, or interruption of or delay in systems, power or telecommunications under third-party control ("**Force Majeure Events**").

11.5 **Notice**. To be effective, any notice required to be given under this Agreement will be given in writing, addressed to the applicable party (at the address in the Order Form) and hand delivered, which is effective upon delivery; sent by reputable overnight courier, which is effective on the business day following deposit with such courier; or sent by the United States mail, first class postage prepaid, which is effective on the third business day after deposit in the United States mail.

11.6 **Governing Law and Venue**. This Agreement will be governed and construed in accordance with the laws of the State of Delaware without giving effect to any principles that may provide for the application of the law of any other jurisdiction. Any legal suit, action or proceeding arising out of or related to this Agreement or the matters contemplated hereunder will be instituted exclusively in the federal courts of the United States or the courts of the State of Delaware, in each case located in the State of Delaware (except where such courts do not have jurisdiction), and each party irrevocably submits to the exclusive jurisdiction of such courts in any such suit, action or proceeding and waives any objection based on improper venue or forum non conveniens. In the event of litigation arising out of this Agreement, the prevailing party will be entitled to its costs and reasonable attorneys' fees.

11.7 **Assignment**. Neither party may assign this Agreement or any right, interest or benefit under this Agreement without the prior written consent of the other party; provided, however, either party may assign this Agreement to a successor who acquires substantially all of the assets or equity of such party through purchase, merger or other transaction without the other party's consent. Any purported assignment in breach of the foregoing will be null and void. This Agreement will be fully binding upon, inure to the benefit of and be enforceable by the parties hereto and their respective successors and permitted assigns, and nothing in this Agreement confers upon any other person or entity any legal or equitable right whatsoever to enforce any provision of this Agreement.

11.8 **Entire Agreement**. This Agreement (together with any Order Forms) constitutes the entire agreement between the parties concerning the subject matter hereof and supersedes all prior and contemporaneous agreements and communications, whether oral or written, between the parties relating to the subject matter hereof, and all past courses of dealing or industry custom. No modification, amendment, or waiver of any provision of this Agreement will be effective unless in a writing duly executed by authorized representatives of both parties. Any standard terms associated with a Customer purchase order or other order document (e.g., general terms and conditions attached to the purchase order form) will be not binding on the parties and of no consequence whatsoever in interpreting the parties' legal rights and responsibilities as they pertain to Services provided under this Agreement. Similarly, any terms required to be accepted electronically through any Customer vendor enrollment, login, invoice submission, or other, process will not apply to this Agreement, are expressly rejected by the parties, and form no basis for any agreement between the parties; notwithstanding any indication of "agreement" to such terms, no such agreement is formed between the parties and the parties acknowledge that only authorized representatives of the parties may enter into agreements between the parties or amendments to this Agreement.

Exhibit A

Data Security

1. PURPOSE AND SCOPE.

This Data Security Exhibit (this "Exhibit") describes data protection and information security standards that Convercent maintains in order to protect Customer Data from unauthorized use, access, disclosure, theft, manipulation, or reproduction. Capitalized terms used but not defined in this Exhibit will have the meaning set forth in the Agreement.

2. DEFINITIONS.

a. "**Applicable Laws and Regulations**" mean any data protection, privacy or information security laws, codes and regulations or other binding restrictions governing Processing of Customer Data, including Personal Data, that are applicable to Convercent's Processing of Customer Data under the Agreement.

b. "**Breach**" or "**Security Breach**" means a compromise (including but not limited to misuse, loss, destruction, or unauthorized access, collection, retention, storage, or transfer) of the systems in which Customer Data has been accessed or acquired by one or more unauthorized parties or any act that violates any Applicable Laws and Regulations.

c. "**Data Center**" means a location at which Convercent Processes Personal Data under this Agreement. Data Centers can be Convercent-owned or third-party service model-based.

d. **“Industry Standard Encryption Algorithms and Key Strengths”** means encryption will at least meet the following standard encryption algorithm (note: The algorithm and key strengths may change depending upon the new and most up-to-date industry standard encryption practice):

- Symmetric encryption: AES (≥ 128-bit);
- Asymmetric encryption: RSA (≥ 2048-bit);
- Hashing: SHA-2 (≥ 224-bit) with “salt” will be added to the input string prior to encoding
to ensure that the same password text chosen by different users will yield different encodings.

e. "**Processing**", "**Processes**" or "**Process**" means any operation or set of operations which is performed upon Customer Data, whether by automatic means or not, including but not limited to collection, recording, organization, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

3. SECURITY MANAGEMENT.

3.1 Scope and Contents. Convercent will develop, implement, maintain and enforce a written information privacy and security program ("**Security Program**") that (i) complies with ISO 27001, SOC 2, HITRUST CFS or an equivalent, (ii) includes administrative, technical and physical safeguards reasonably designed to protect the confidentiality, integrity and availability of Customer Data and (iii) is appropriate to the nature, size and complexity of Convercent's business operations; and (iv) complies with any Applicable Laws and Regulations.

a. Security Program Changes. Convercent will provide details of any major changes to its Security Program that may adversely affect the security of any Customer Data.

b. Security Officer. Convercent will designate a senior employee to be responsible for overseeing and carrying out its Security Program and for communicating with Customer on information security matters ("**Convercent's Security Officer**"). Upon Customer's request, Convercent's Security Officer will provide Customer with the contact information of one or more Convercent representatives who will be available to discuss any security concerns (e.g., discovered vulnerability, exposed risk, reported concern) with Customer and to communicate the level of risk associated with such concerns and any remediation thereof.

3.2 Personnel Security.

a. Verification Checks. Prior to assigning any of its Personnel to positions in which they will, or Convercent reasonably expects them to, have access to Customer Data, Convercent will conduct or verify background checks on such Personnel, except where expressly prohibited by law. For the purposes of this Exhibit, "**Personnel**" means Convercent's employees, independent contractors, and subcontractors that have access to Personal Data.

b. Training. Convercent Personnel will, upon hiring, and at least annually thereafter, participate in security awareness training. This training will cover, at a minimum, Convercent's security policies, including acceptable use, password protection, data classification, Breach reporting, the repercussions of violations, and brief overviews of Applicable Laws and Regulations.

c. Due Diligence over Subcontractors. Convercent maintains a security process to conduct appropriate due diligence prior to utilizing subcontractors to provide any of the Services. Convercent will assess the security capabilities of any such subcontractors on an annual basis to ensure subcontractor's ability to comply with this Exhibit and the terms of the Agreement. The due diligence process will provide for the identification and resolution of significant security issues prior to engaging a subcontractor, written information security requirements that require subcontractor to adhere to Convercent's key information security policies and standards within all contracts, and for the identification and resolution of any security issues during the term of the Agreement.

4. PHYSICAL SECURITY.

4.1 General. The physical security processes in this Section apply to all facilities used to provide the Services at which Customer Data is accessed, processed, stored, transferred or maintained, including any floor space where Services are performed in which Personnel have access to Customer Data and servers or other equipment that processes or stores Customer Data (the "**Secure Area**").

4.2 Secure Area. Customer Data will only reside within a Secure Area. Convercent will restrict access to and will control and monitor all physical areas in Convercent's premises that contain Customer Data. Convercent will secure and monitor access to any Secure Area and will maintain physical security controls at the Secure Area, on a 24-hours-per-day, 7-days-per-week basis ("**24/7**"). Convercent will revoke any Personnel's access to Secure Areas within twenty-four (24) hours of the cessation of such Convercent Personnel's need to access buildings, system(s) or application(s).

4.3 Data Centers. To the extent Convercent is operating a Data Center or utilizing a Third-Party Data Center, Convercent will comply with physical security controls outlined in industry standards such as ISO 27001, SSAE 16 or ISAE 3402, or PCI-DSS. All access to areas, cabinets, or racks that house telecommunications, networking devices and other "data transmission lines" or equipment will be controlled as follows:

a. access will be controlled by badge reader at one or more entrance points;

b. doors used only as exit points will have only "one way" doorknobs or crash bar exit devices installed;

c. all doors will be equipped with door alarms contacts;

d. all exit doors will have video surveillance capability; and

e. all card access and video surveillance systems will be tied into generator or UPS backup systems.

5. Logical Security.

5.1 General. The logical security processes in this Section apply to all Convercent's systems or Convercent's agents' or its assigns' systems and supporting networks used to provide the Services on which Customer Data is accessed, processed, stored, transferred or maintained.

5.2 Systems Access Control and Network Access Control.

a. Access Controls. Convercent employs access control mechanisms that:

   i. prevent unauthorized access to Customer Data;

   ii. limit access to Personnel with a business need to know;

   iii. follow principle of least privilege allowing access to only the information and resources that are necessary under the terms of the Agreement; and

   iv. have the capability of detecting, logging, and reporting access to the system or network or attempts to breach security of the system or network.

b. Accounts. All Personnel must have an individual account that authenticates that individual's access to Customer Data. Convercent does not allow sharing of accounts. Access controls and passwords are configured in accordance with industry standards and best practices. Passwords will be hashed with industry standard algorithms per the Storage, Handling and Disposal Section, below.

c. Regular Review of Access Controls. Convercent maintains a process to review access controls on a minimum annual basis for all Convercent systems that contain Customer Data, including any system that, via any form of communication interface, can connect to the system on which Customer Data is stored. These access processes and the process to establish and delete individual accounts will be documented in, and will be in compliance with, Convercent's security policies and standards referenced in the Security Management: Scope and Contents Sub-section, above. Convercent maintains the same processes of review and validation for any third party hosted systems it uses that contain Customer Data.

d. Remote Access Authentication. Convercent will configure remote access to all networks storing or transmitting Customer Data to require two-factor authentication for such access or at a minimum will use access control lists to only allow connectivity to such networks from Convercent's own network.

e. Revocation of Access. Convercent will revoke Personnel's access to physical locations, systems, and applications that contain or process Customer Data within twenty-four (24) hours of the cessation of such Personnel's need to access the system(s) or application(s).

5.3 Telecommunication and Network Security.

a. Convercent will deploy reasonably appropriate firewall technology in the operation of Convercent's sites. Traffic between Customer and Convercent will be protected and authenticated by industry standard cryptographic technologies. Specifically, firewall(s) must be able to effectively perform the following functions: stateful inspection, logging, support for all IPSec standards and certificates, support for strong encryption and hashing, ICMP and SNMP based monitoring and anti-spoofing.

b. Firewall Maintenance. At a minimum, Convercent will review firewall rule sets annually to ensure that legacy rules are removed and active rules are configured correctly.

c. Intrusion Detection and Prevention. Convercent will deploy intrusion detection or preferably prevention systems (NIDS/NIPS) in order to generate, monitor, and respond to alerts which could indicate potential compromise of the network and/or host.

d. Log Management. Convercent will deploy a log management solution and retain logs produced by firewalls and intrusion detection systems for a minimum period of one (1) year.

e. Network Segmentation. Convercent will establish and maintain appropriate network segmentation, including the use of virtual local area networks (VLANS) where appropriate, to restrict network access to systems storing Customer Data. Convercent will proxy all connections from public networks into Convercent's internal network using DMZ or equivalent. Convercent will not allow direct connections from public networks into any network segment storing Customer Data.

5.4 Malicious Code Protection.

a. All workstations and servers will run the current version of industry standard anti-virus software with the most recent updates available on each workstation or server. Virus definitions must be updated within twenty-four (24) hours of release by the anti-virus software vendor. Convercent will configure this equipment and have supporting policies to prohibit users from disabling anti-virus software, altering security configurations, or disabling other protective measures put in place to ensure the safety of Customer's or Convercent's computing environment.

b. Convercent will have current anti-virus software configured to run real-time scanning of machines and a full system scan on a regularly scheduled interval not to exceed seven (7) calendar days.

c. Convercent will scan incoming and outgoing content for malicious code on all gateways to public networks, including, but not limited to, email and proxy servers.

d. Convercent will quarantine or remove files that have been identified as infected and will log the event.

5.5 Data Loss Prevention. Convercent will employ a system to prevent the inadvertent or intentional compromise of Customer Data. Controls must exist to track activity, inspect network traffic, including email and other protocols, and filter/block certain user actions to ensure Customer Data remains secured.

6. Systems Development and Maintenance.

6.1 Documentation. Convercent will maintain documentation on overall system, network, and application architecture, data flows, process flows, and security functionality for all applications that process or store any Customer Data.

6.2 Change Management. Convercent will employ an effective, documented change management program with respect to the Services as an integral part of its security profile. This includes logically or physically separate environments from production for all development and testing. No Customer Data will be transmitted, stored or processed in an environment that does not maintain at least the minimum administrative, technical and physical safeguards as described in this Exhibit.

6.3 Vulnerability Management and Application Security Assessments. Convercent will run internal and external network vulnerability scans at least quarterly and after any material change in the network configuration (e.g., new system component installations, changes in network topology, firewall rule modifications, or product upgrades). Vulnerabilities identified and rated as high risk by Convercent will be remediated within ninety (90) days of discovery.

1. For all Internet-facing applications that collect, transmit or display Customer Data, Convercent agrees to conduct an application security assessment review to identify common security vulnerabilities as identified by industry-recognized organizations (e.g., OWASP Top 10 Vulnerabilities; CWE/SANS Top 25 vulnerabilities) annually or for all major releases, whichever occurs first. The scope of the security assessment will primarily focus on application security, including, but not limited to, a static code analysis or penetration test of the application, as well as a code review. At a minimum, it will cover the OWASP Top 10 vulnerabilities (https://www.owasp.org).

2. Convercent may utilize a qualified third party to conduct the application security assessments. Convercent may conduct the security assessment review themselves, provided that Convercent's Personnel performing the review are sufficiently trained, follow industry standard best practices, and the assessment process is reviewed and approved by Customer. Vulnerabilities identified and rated as high risk by Convercent will be remediated within ninety (90) days of discovery.

6.4 Source code review. Convercent will have a documented program for source code reviews and maintain documentation of secure code reviews performed for all applications that store or process Customer Data.

6.5 Patch Management. Convercent will patch all workstations and servers with all current operating system, database and application patches deployed in Convercent's computing environment according to a schedule predicated on the criticality of the patch. Convercent will perform appropriate steps to help ensure patches do not compromise the security of the information resources being patched. All emergency or critical rated patches must be applied as soon as possible but at no time will exceed six weeks from the date of release.

7. Email Security. If Convercent is sending emails to Customer customers or employees, appropriate email identity solutions, including but not limited to DKIM, SPF, and DMARC, will be utilized.

8. Customer Security Assessments and Audits.

8.1 Convercent agrees, upon written request no more than on an annual basis, to allow its procedures and documentation to be inspected by Customer (or its designee) in order to ascertain compliance with Applicable Laws and Regulations, this Exhibit, or any non-disclosure agreements and any agreements between Customer and Convercent.

8.2 Convercent will reasonably cooperate with audit requests by providing access to relevant knowledgeable personnel, documentation, and application software.

9. BREACH NOTIFICATION AND RESPONSE PROCEDURES.

9.1 **Notification**. Convercent will maintain an incident response function capable of identifying, mitigating the effects of, and preventing the recurrence of, Security Breaches. Upon discovering or otherwise becoming aware a Breach, Convercent will take all reasonable measures to mitigate the harmful effects of the Breach. Convercent will also notify Customer of the Breach as soon as practicable, but in no event later than 48 hours after the Breach. Notice to Customer will include: (i) the identification of the Customer Data which has been or Convercent reasonably believes has been used, accessed, acquired or disclosed during the incident; (ii) a description of what happened, including the date of the incident and the date of discovery of the incident, if known; (iii) the scope of the incident, including a description of the type of Customer Data involved in the incident; (iv) a description of Convercent's response to the incident, including steps Convercent has taken to mitigate the harm caused by the incident; and (v) other information as Customer may reasonably request and is reasonably applicable. Convercent agrees to cover the costs of any such notification, including reimbursing Customer for any reasonable costs.

9.2 **Response**. Convercent will retain all data related to known and reported Breaches or investigations until Convercent reasonably determines that the data is no longer needed. Upon Customer's request, Convercent will permit Customer or its third-party auditor to review and verify relevant video surveillance records, access logs and data pertaining to any Breach investigation. Upon conclusion of investigative, corrective, and remedial actions with respect to a Breach, Convercent will prepare and deliver to Customer a final report that describes in detail: (i) the extent of the Breach; (ii) the Customer Data disclosed, destroyed, or otherwise compromised or altered; (iii) all supporting evidence, including, but not limited to, system, network, and application logs; (iv) all corrective and remedial actions completed; and (v) all efforts taken to mitigate the risks of further Breaches.

10. STORAGE, HANDLING AND DISPOSAL.

10.1 **Data Segregation**. Convercent will physically or logically separate and segregate Customer Data from its other clients' data.

10.2 **Electronic Form Data**. Convercent will utilize Industry Standard Encryption Algorithms and Key Strengths (as defined in the Definitions Section of this Exhibit) to encrypt the following:

a. All Customer Data that is in electronic form while in transit over all public wired networks (e.g., Internet) and all wireless networks;

b. All Customer Data stored in databases, in file systems, and on various forms of online and offline media (DASD, tape, etc.);

c. Passwords for privileged access will be hashed with irreversible industry standard algorithms with randomly generated "salt" added to the input string prior to encoding to ensure that the same password text chosen by different users will yield different encodings. The randomly generated salt will be at least as long as the output of the hash function; and

10.3 **Key Management**. Where encryption is utilized, Convercent will maintain a key management process that meets the following minimum requirements:

1. At least one key custodian must be officially designated.

2. Key custodians must ensure that all keys used in a storage encryption solution are secured and managed properly to support the security of the solution.
3. Key management must be planned to include secure key generation, use, storage, and revocation.
4. Key management practices must support the recovery of encrypted data if a key is inadvertently disclosed or destroyed or becomes unavailable.
5. Key custodians must ensure that access to encryption keys is properly restricted to approved administrators. Private keys must not be stored on the same media and/or virtual instance as the data they protect.
6. Authentication must be required in order to gain access to keys.
7. Keys will be rotated annually and must be replaced before they expire.

10.4 Physical Form Data. Convercent will only store Customer Data in physical form in a Secure Area, and Convercent will establish and operate a document control system to record and track the transfer of all Customer Data that is in physical form both (i) between and within Convercent facilities, and (ii) via any external shipment. Such a control system will include, at minimum, a description of the specific records being transferred (e.g., customer or employee records, etc.), as well as the parties who are preparing, shipping, receiving, and processing such materials.

10.5 Shipments. Convercent will transfer all Customer Data in physical form (i.e. external hard drives, backup tapes, etc.) in secure containers or packaging. Convercent will ship any Customer Data in physical form via controlled transportation methods reasonably designed to prevent unauthorized access or compromise, including encryption of electronic media where applicable. Controlled transportation methods include enclosed locked vehicles, registered mail, and commercial shipping services with numbered tracking capability (e.g., UPS, FedEx).

10.6 Data Retention. Except where prohibited by law, upon (i) the date of expiration or termination of the Agreement; (ii) when Customer Data is no longer required for the purposes of the Agreement; or (iii) at any time upon written request from Customer, whichever occurs earliest:

a. Convercent will promptly remove the Customer Data from Convercent's database and destroy it within a reasonable timeframe, but in no case longer than thirty (30) days thereafter; and
b. Convercent will provide Customer with a written certification regarding such removal and destruction upon request.

11. BUSINESS CONTINUITY AND DISASTER RECOVERY.

Convercent will set up a Business Continuity Management program that meets the needs of the business and Services being provided to Customer. To that end, a minimum level of crisis management, business continuity, and disaster recovery planning will be completed by Convercent.

a. Business Continuity, and Disaster Recovery Plans will be as follows:

   - A Business Continuity Plan includes, but is not limited to, elements such as event management, life safety, business recovery, alternative site locations, and call tree testing.

   - A Disaster Recovery Plan includes, but is not limited to, infrastructure, technology, and system(s) details, recovery activities, and identifies the people / teams required for such recovery.

b. Plan Content. The Business Continuity Plan and Disaster Recovery Plan will address actions that Convercent will take in the event of an extended outage of Service and will include test results for the

Business Continuity and Disaster Recovery Plan from a test performed annually. Convercent will ensure that its plans address the actions and resources required to provide for (i) the continuous operation of Convercent, and (ii) in the event of an interruption, the recovery of the functions required to enable Convercent to provide the Services described in the Agreement, including all required systems, hardware, software, resources, personnel and data supporting these functions, within a time period time sufficient to meet service levels described in the Agreement.

12. **SURVIVAL**. Convercent's obligations and Customer's rights under this Exhibit will become effective on the Effective Date of the Agreement and will continue in effect so long as Convercent possesses Customer Data.

13. **CONFLICT**. If and to the extent language in this Exhibit or any of its Schedule conflicts with the Agreement, this Exhibit will control.

Data Processing Addendum

This Data Processing Addendum (the "DPA") is between Convercent, Inc. ("Convercent" or "Processor") and the customer identified below ("Customer"), and forms a part of, and is incorporated into, the Master Services Agreement (the "Agreement") between Convercent and Customer. All capitalized terms not defined herein shall have the meaning set forth in the Agreement. The parties agree as follows:

1. Definitions

1.1 "Applicable Data Protection Laws" means the data protection laws, rules and regulations that are applicable to Convercent. With respect to EU Personal Data "Applicable Data Protections Law(s)" shall include, but not be limited to, the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679).

1.2 "Customer EU Personal Data" means Customer Personal Data about individuals who are, based on information known to Processor, residents of the European Union.

1.3 "Customer Personal Data" means Personal Data received by Convercent pursuant to this Agreement and pertaining to Customer's current, former, or potential customers, employees, vendors, or other individuals.

1.4 "Data Security Exhibit" means the data security terms contained in the Agreement, which may be attached thereto as Exhibit A.

1.5 "Data Subject" means the identified or identifiable person to whom Personal Data relates.

1.6 "EU" or "European Union" means the European Union inclusive of Switzerland and the United Kingdom, whether or not the United Kingdom has officially withdrawn from the European Union.

1.7 "Personal Data" shall have the meaning assigned to the terms "personal data" or "personal information" under Applicable Data Protection Laws.

1.8 "Process", "Processes", "Processing", "Processed" shall have the meanings assigned to them in the Applicable Data Protection Laws.

1.9 "Security Incident" means an event about which Convercent knows, discovers, is notified of, or reasonably suspects that Customer Personal Data has been accessed, disclosed, acquired or used by unauthorized persons, in violation of Applicable Data Protection Laws.

1.10 "Sub-Processor" means Convercent's contractors, agents, vendors, and third-party service providers, that Process Customer Personal Data.

2. Data Handling and Access

2.1 **General Compliance**. Customer hereby authorizes and instructs Processor, and Processor will, and will require Sub-Processors, to Process Customer Personal Data in compliance with the terms of the Agreement, this DPA, the Data Security Exhibit, and all Applicable Data Protection Laws. Customer represents and warrants that it has all authority, grounds, rights, and consents necessary to enable Convercent to Process the Customer Personal Data as required by the Agreement, in accordance with the Applicable Data Protection Laws.

2.2 **Convercent and Sub-Processor Compliance.** Convercent agrees to (i) enter into a written agreement with Sub-Processors regarding such Sub-Processors' Processing of Customer Personal Data that imposes on such Sub-Processors data protection and security requirements for Customer Personal Data that are compliant with Applicable Data Protection Laws, that are consistent with the requirements under this DPA and that, at a minimum, require a level of data protection and security equal to or superior to the level of data protection and security under this DPA; (ii) reasonably enforce compliance with such written agreement; and (iii) remain responsible to Customer for the actions or omissions of Convercent's Sub-Processors (and their sub-processors if applicable) with respect to the Processing of Customer Personal Data.

2.3 **Authorization to Use Sub-Processors**. Customer hereby authorizes (i) Convercent to engage Sub-Processors and (ii) Sub-Processors to engage sub-processors. Convercent will provide Customer, upon Customer's request, the name, address and role of each Sub-Processor used to Process Customer Personal Data and any other records of Processing of Customer Personal Data that Sub-Processors are required to maintain and provide under Applicable Data Protection Laws. Customer hereby approves of the following Sub-Processors: Datavail (United States, India), Microsoft (Europe), Amazon Web Services (Europe), Google Cloud Platform (Europe), Five Star Call Centers (United States) and Acquia (United States or Europe).

2.4 **Objection Right for New Sub-Processors**. Convercent will inform Customer of any new Sub-Processor before authorizing such new Sub-Processor to Process Personal Data in connection with the provision of the applicable Services. Customer may object to Convercent's use of a new Sub-Processor by notifying Convercent promptly in writing within ten (10) business days after receipt of such information. In the event Customer objects to a new Sub-Processor, as permitted in the preceding sentence, Convercent may address the concerns with respect to the Sub-Processor, 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-to Sub-Processor without unreasonably burdening the Customer. If Convercent does not do so within a reasonable period of time, which shall not exceed thirty (30) days, Customer may terminate the applicable Order Form(s) with respect only to those Services which cannot be provided by Convercent without the use of the objected-to new Sub-Processor by providing written notice to Convercent. Convercent will refund Customer any prepaid fees covering the remainder of the term of such Order Form(s) following the effective date of termination with respect to such terminated Services.

2.5 **Following Instructions**. Processor will Process Customer Personal Data only in accordance with the written instructions of Customer, which instructions include Processing for the following purposes: (i) Processing in accordance with the Agreement and applicable Order Form(s); (ii) Processing initiated by users in their use of the Services; (iii) Processing to further develop and provide services for Convercent customers (provided that no Customer Personal Data is disclosed to any other customer in breach of any confidentiality obligation), and (iv) Processing to comply with other documented reasonable instructions provided by Customer (e.g., via email) where such instructions are consistent with the terms of the Agreement and all Applicable Data Protection Laws.

2.6 **Details of the Processing**. The subject matter of Processing of Personal Data by Convercent is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Schedule 1 (Details of the Processing) to this DPA.

3. Rights of Data Subjects

Convercent will, to the extent legally permitted, promptly notify Customer if Convercent receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure (“right to be forgotten”), data portability, objection to the Processing, or its right not to be subject to an automated individual decision making (“Data Subject Request”). Convercent will assist Customer by appropriate technical and organizational measures, insofar as this is possible and to the extent that the Services do not already provide such measures for Customer, for the fulfilment of Customer’s obligation to respond to a Data Subject Request under Applicable Data Protection Laws. In addition, to the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, Convercent will, upon Customer’s request and at Customer’s expense, provide commercially reasonable efforts to assist Customer in responding to such Data Subject Request, to the extent Convercent is legally permitted to do so and the response to such Data Subject Request is required under Data Protection Laws and Regulations. To the extent legally permitted, Customer will be responsible for any reasonable costs arising from Convercent’s provision of such assistance.

4. EU - U.S. Compliance. This Section applies where the Processor Processes Customer EU Personal Data.

4.1 Convercent Data Transfer Mechanism. The parties hereby incorporate the Standard Contractual Clauses approved by the European Commission as Schedule 2. If the European Commission approves an alternative to the Standard Contractual Clauses, Convercent may rely on such alternative instead of the Standard Contractual Clauses. To the extent there is any conflict between the body of this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall control.

4.2 Prior Consultation. Processor agrees to provide reasonable assistance to Customer (at Customer’s expense) where, in Customer’s judgement, the type of Processing performed by Processor is likely to result in a high risk to the rights and freedoms of natural persons (e.g., systematic and extensive profiling, Processing sensitive Personal Data on a large scale and systematic monitoring on a large scale, or where the Processing uses new technologies) and thus requires a data protection impact assessment and/or prior consultation with the relevant data protection authorities.

4.3 Demonstrable Compliance. Processor agrees to keep records of its Processing in compliance with Applicable Data Protection Laws and provide such records to Customer upon request. If Processor is collecting Customer EU Personal Data on Customer’s behalf, such records may include, to the extent reasonably requested by Customer, records of the verifiable consent under Applicable Data Protection Laws.

5. Information Security

5.1 Controls for the Protection of Data. Convercent will maintain appropriate technical and organizational measures for protection of the security, confidentiality and integrity of Personal Data, as set forth in the Data Security Exhibit. Convercent regularly monitors compliance with these measures. Convercent will not materially decrease the overall security of the Services during the term.

5.2 Third-Party Certifications and Audits. Convercent has obtained the third-party certifications and audits set forth in the Data Security Exhibit. Upon Customer’s written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, Convercent will, if Customer is not a competitor of Convercent, make available to Customer (or a reasonably acceptable independent, third-party auditor) a copy of Convercent's then most recent third-party audits or certifications, as applicable.

6. Assessments, Audits and Remediation

6.1 Assessments. Records to demonstrate compliance with this DPA and Applicable Data Protection Laws will be maintained by Convercent and provided to Customer upon request. Convercent will complete within two weeks any reasonable data protection questionnaire provided by Customer.

6.2 Audits. For the purpose of verifying Convercent's compliance with Applicable Data Protection Laws and the Agreement and upon reasonable notice of no less than thirty (30) days, Convercent agrees to permit Customer, at Customer's cost and no more than once annually unless legally required, to conduct audits through a Convercent approved or certified third party auditor. However, Convercent agrees to allow audits to be conducted directly by Customer where, under Applicable Data Protection Laws, (a) Customer has the right to conduct audits directly; and (b) such right cannot be contractually waived by Customer. Convercent agrees to cooperate in good faith with the audit and promptly (i) provide access to books, records (including, but not limited to, security scan records), and other information necessary for the audit, and (ii) at Customer's request enable access to Convercent's premises if absolutely necessary to properly conduct the audit or required under Applicable Data Protection Laws. Notwithstanding the forgoing, Customer may not conduct any security scans or other intrusion testing on Convercent's systems without the express prior written consent of Convercent. Customer agrees to (x) schedule audits to minimize disruption to Convercent's business, (y) require any third party it employs to sign a non-disclosure agreement, and (z) make the results of the audit available to Convercent. Customer will only disclose the results of the audit to third parties if such disclosure is (A) required to demonstrate Customer's own compliance, or (B) otherwise required under applicable laws.

6.3 Remediation. Convercent agrees to promptly take action to correct any documented material security issue affecting Customer Personal Data identified by such audit and to inform Customer of such actions. If action is not promptly taken, Customer's sole remedy will be to terminate the Agreement and any or all Order Forms at Customer's discretion provided that Convercent will incur no penalty for any such termination.

7. Secure Disposal

Customer Personal Data will be securely disposed (i) during the duration of the Agreement upon Customer's written request if such Customer Personal Data is no longer reasonably required to perform the services, (ii) at the termination of the provision of the services. If instructed by Customer, a copy of such Customer Personal Data will be returned to Customer prior to disposal. Convercent may retain Customer Personal Data to the extent that it is required to do so under Applicable Data Protection Laws. Notwithstanding the forgoing, Convercent may store copies of Customer Personal Data in its encrypted backups in accordance with its data retention policies where storage will not exceed 365 days and where such storage is required by law.

8. Changes to Requirements

The parties will work together in good faith to amend or supplement this DPA from time to time to reflect new requirements under Applicable Data Protection Laws.

9. Security Incident

9.1 Policy. Convercent maintains Security Incident management policies and procedures specified in the Data Security Exhibit and will, to the extent required under Applicable Data Protection Laws, notify Customer without undue delay after becoming aware of any Security Incident. Convercent will make reasonable efforts to identify the cause of such Security Incident and take those steps as Convercent deems necessary and reasonable in order to remediate the cause of such Security Incident to the extent the remediation is within Convercent's reasonable control. The obligations herein shall not apply to Security Incidents that are caused by Customer or Customer's Users.

9.2 Reports. Upon request by Customer, Convercent will enable Customer to review the results of and reports relating to the investigation and response to a Security Incident.

10. Termination Obligations

10.1 Termination. Notwithstanding anything to the contrary in the Agreement or this DPA, Customer may terminate the Agreement or any portion thereof immediately upon written notice to Convercent, and without judicial notice or resolution or prejudice to any other remedies, in the event a data protection or other regulatory authority or other tribunal or court in any country finds there has been a breach of Applicable Data Protection Laws by virtue of Customer's or Convercent's Processing of Customer Personal Data in connection with the Agreement, and such breach has not been cured within sixty (60) days of the breaching party receiving notice thereof.

10.2 Effect of Termination or Expiration. Customer Personal Data will be securely destroyed unless Convercent is required to retain such information under Applicable Data Protection Laws. Convercent's obligations to protect Customer Personal Data will continue until all such information has been permanently and completely destroyed or deleted, including from any back-up.

11. Contact Information

Convercent will designate a point of contact as its Privacy and Security Coordinator. This Privacy and Security Coordinator will: (i) maintain responsibility for applying adequate protections to Customer Personal Data, including the development, implementation, and maintenance of its information security program, (ii) oversee application of Convercent compliance with the requirements of this DPA, and (iii) serve as a point of contact for internal communications and communications with Customer pertaining to this DPA and compliance with or any breaches thereof.

[signature page follows]

To evidence the parties' agreement to this Data Processing Addendum, they have executed it on the date listed below by the Customer.

CONVERCENT		**CUSTOMER**	
Signature	______________________	**Signature**	______________________
Name:	______________________	**Name:**	______________________
Title:	______________________	**Title:**	______________________
Date:	______________________	**Date:**	______________________
Address:	3858 Walnut St Suite #255, Denver, CO 80205	**Address:**	______________________

SCHEDULE 1

Nature and Purpose of Processing

Convercent will Process Personal Data as necessary to perform the Services pursuant to the Agreement, as further specified in the Order Form, and as further instructed by Customer in its use of the Services.

Duration of Processing

Subject to Section 7 of the DPA, Convercent will Process Personal Data for the duration of the Agreement, as provided in the DPA, and as otherwise agreed upon in writing.

Categories of Data Subjects

Third parties or Customer may submit Personal Data to the Services, the extent of which is neither determined nor controlled by Convercent, and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Clients, business partners and vendors of Customer (who are natural persons)
- Employees, officers, directors, contractors or contact persons of Customer's third-party suppliers, business partners and vendors
- Customer users authorized by Customer to use the relevant Services
- Any third party making a report through the Services regarding Customer

Type of Personal Data

Third parties or Customer may submit Personal Data to the Services, the extent of which is neither determined nor controlled by Convercent, and which may include, but is not limited to the following categories of Personal Data:

- Contact details (e.g. name, postal address, job title, job position, location, employer, relationship with the organization, e-mail address, telephone number, postal address);
- Username and password for the account of data subjects may establish in the relevant Services;
- For whistle-blower hotline reports, in addition to the foregoing, the following may also be captured:
    - facts reported by a reporter about a suspected violation, including how and where the suspected violation occurred and how the reporter learned about the suspected violation;
    - identity, function and contact details of individuals allegedly involved in the suspected violation;
    - Photographs, videos, comments, and other content or information data subjects may submit to the relevant Services.

Special categories of data (if appropriate)

Personal Data may concern the following special categories of data:

- 'Whistleblowing' reports could, theoretically, include reference to an individual's race or ethnic origin, political opinion, religious or philosophical belief, trade union membership, health, sex life or sexual orientation.
- Allegations or concerns could, theoretically, also refer to criminal convictions or offences.

SCHEDULE 2

STANDARD CONTRACTUAL CLAUSES

Standard Contractual Clauses (processors)

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

Name of the data exporting organization: ______________________________

Address: ______________________________

Telephone: ______________ **Fax**: ______________ **Email**: ____________________

Other information needed to identify the organization:

____

(the data exporter)

And

Name of the data importing organization: Convercent, Inc.

Address: 3858 Walnut Street, #255, Denver, CO 80205 USA

Telephone: 303.526.7600 **Fax**: 303.526.7757 **Email**: security@convercent.com

Other information needed to identify the organisation:

Convercent, Inc. (“Convercent”)

(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:

(a) *'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;

(b) '*the data exporter'* means the controller who transfers the personal data;

(c) *'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;

(d) *'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;

(e) '*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;

(f) *'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

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:

(i) 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,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) 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;

(f) 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;

(g) 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;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) 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 of 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):

Signature ____________________

(stamp of organisation)

On behalf of the data importer:

Name (written out in full): Convercent, Inc.

Position: CFO

Address: 3858 Walnut Street, #255, Denver, CO 80205 USA

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

Signature ____________________

(stamp of organisation)

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

(i) the legal entity that has executed the Standard Contractual Clauses as a data exporter and, (ii) all affiliates (as defined in the Agreement) of Customer established in the European Economic Area (EEA) and Switzerland that have purchased Services on the basis of one or more Agreements or Order Form(s).

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

a provider of a Software as a Service ("SaaS") cloud computing solutions for its clients ("data exporter" or "data controller") that processes personal data upon the instruction of the data exporter in accordance with the terms of the Agreement. If applicable to the data exporter's Agreement, employees of the data exporter can report incidents through an EU/Swiss equivalent to an 800 number or through the data importer SaaS application.

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

Employees, officers, directors, vendors, contractors and other related or third parties working with or for data exporter.

Categories of data

The personal data transferred concern the following categories of data (please specify):

Contact details (e.g., name, postal address, email address, and telephone number); Username and password for the account of data subjects may establish in our application; Photographs, videos, comments, and other content or information data subjects may submit to data importer through the application.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

Although the data importer has advised the data exporter against including any sensitive data in the personal data that is transferred, reporting individuals can include any information they choose. The data exporter controls such data in its sole discretion.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

Personal data may be transferred through a third party hosted cloud environment, through data importer's call center if submitted telephonically or through SFTP or API protocols. All transfers shall be in accordance with the Agreement.

DATA EXPORTER

Name: ____________________

Authorised Signature ____________________

DATA IMPORTER

Name: Convercent, Inc.

Authorised Signature ____________________

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties

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):

Appendix 2 to the Standard Contractual Clauses (Convercent as Data Importer)

1. **Physical Access control (to data processing systems):**
   Measures to prevent unauthorised persons from obtaining physical access to the data processing systems with which personal data are processed.

   - The data center buildings are controlled by Azure and Amazon Web Services. Both partners are ISO 27001 and SOC 2 Certified

2. **Access control (to use of data processing systems and methods):**
   Measures to prevent data processing systems and methods from being used by unauthorised persons.

   - Complex passwords are enforced with system policy and expiration times appropriate to the level of access. Privileged accounts have more stringent controls including short life passwords with enterprise level management

   - Accounts are locked for invalid attempts to log on and audit trails are logged and monitored for inappropriate and un-authorized activity

   - Role based authentication is used where possible with auditing processes and activities to manage appropriateness of access. Privileged accounts utilize two-factor authentication with enterprise level management where required.

   - Data systems are encrypted in transit using HTTPS and at rest using Microsoft SQL TDE.

   - Strict Firewall rules are established only allowing required access to and from the production environment

   - Internal data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process personal data.

   - The Data Importer designs its systems to: (i) only allow authorized persons to access data they are authorized to access; and (ii) ensure that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording. The systems are designed to detect any inappropriate access.

   - These mechanisms are designed to grant only approved access rights to site hosts, logs, data and configuration information. The granting or modification of access rights must also be in accordance with the Data Importer's internal data access policies and training. Approvals are managed by workflow tools that maintain audit records of all changes. Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication (e.g., login to workstations), password policies that follow at least industry standard practices are implemented.

3. **Access control (to data)**:
   Measures to ensure that persons who are authorised to use a data processing method only have access to that personal data to which their access authorisation applies and that this data cannot be read, copied, modified or removed during processing without authorization.

   - User accounts are unique and assigned to appropriate groups by administrative personnel for control

   - Roles limit access to objects through an authorization process with appropriate audit trails

   - Audit logs are monitored for activity and access appropriateness

   - System policies and procedures protect data during processing for appropriate access by authorized personnel

   - All changes to access are logged and reviewed during periodic audits. Abnormal changes create alerts to appropriate personnel

4. **Disclosure controls:**
   Measures designed to ensure that personal data cannot be read, copied, modified or removed during electronic transmission, data transport or storage on data carriers without authorisation.

   - Industry standard practices are employed to protect data in transit. Private Networks, Virtual Private Networks and Secure Socket Layer technologies are used to prevent unauthorized access

   - Logging of system access is monitored and reviewed for appropriateness

5. **Input controls:**
   Measures to ensure that it is possible to retroactively check and verify whether, when and by whom data has been entered into, modified or removed from the data processing system.

   - Our access and activity logs are monitored and have alert triggers for unauthorized or inappropriate activity as well as provide change history

6. **Control of instructions:**
   Measures to ensure that personal data are processed solely in accordance with the instructions of the Client.

   - Corporate compliance and security policies highlight that client data is accessed only with a business need and is not disclosed

7. **Availability control:**
   Measures to ensure that personal data are protected from accidental destruction or loss.

- Systems are backed up daily to enable recovery of data on a schedule determined by policy

- High availability or recovery technologies are employed to maintain system operation, availability and redundancy

- Production environments are replicated in geographically separated data centers with remote storage of backups and recovery systems

- Our infrastructure includes state-of-the-art firewall, anti-malware, and malicious activity detection technology

- Our Disaster Recovery Plans are documented, reviewed and tested on a regular basis

8. **Separation controls:**
   Measures to ensure that personal data that is stored for separate purposes is processed separately.

   - We have a tiered development, testing, stage and production environment to separate function and operation

   - Access controls are employed to segregate the environments

9. Personnel:

- The Data Importer's personnel are required to conduct themselves in a manner consistent with the company’s guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. The Data Importer conducts reasonably appropriate backgrounds checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations.

- Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, the Data Importer’s confidentiality and privacy policies. Personnel are provided with security training.

10. Subprocessor Security:

- Prior to onboarding Subprocessors, the Data Importer conducts an audit of the security and privacy practices of Subprocessors to ensure Subprocessors provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once the Data Importer has assessed the risks presented by the Subprocessor, the Subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms.