MASTER SERVICES AGREEMENT

THIS MASTER SERVICES AGREEMENT (THIS **"AGREEMENT"**) IS BY AND BETWEEN ASYMBL, INC., A DELAWARE CORPORATION ("**ASYMBL**"), TOGETHER WITH ITS AFFILIATES (AS THAT TERM IS DEFINED IN THIS AGREEMENT) (ASYMBL AND AFFILIATES, COLLECTIVELY AND INDIVIDUALLY, THE **"PROVIDER"**) AND THE CUSTOMER IDENTIFIED ON THE ORDER FORM AS THE LICENSEE OF THE PRODUCTS AND/OR RECIPIENT OF THE SERVICES.

AS USED IN THIS AGREEMENT, (I) THE TERM "**AFFILIATES**" MEANS ANY CORPORATION OR OTHER BUSINESS ENTITY THAT OWNS AND CONTROLS, OR IS OWNED AND CONTROLLED BY, OR IS UNDER COMMON OWNERSHIP AND CONTROL WITH PROVIDER, INCLUDING BUT NOT LIMITED TO BLUEPRINT ADVISORY SOFTWARE, LLC, A DELAWARE LIMITED LIABILITY COMPANY, (FOR THE PURPOSE OF THIS CLAUSE, OWNERSHIP AND CONTROL SIGNIFIES OWNERSHIP OF A MAJORITY OF THE VOTING RIGHTS IN A BUSINESS ENTITY), (II) THE TERM **"CUSTOMER"** MEANS IN THE CASE OF AN INDIVIDUAL ACCEPTING THIS AGREEMENT ON HIS OR HER OWN BEHALF, SUCH INDIVIDUAL, OR IN THE CASE OF AN INDIVIDUAL ACCEPTING THIS AGREEMENT ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, THE COMPANY OR OTHER LEGAL ENTITY ON BEHALF OF WHICH SUCH INDIVIDUAL IS ACCEPTING THIS AGREEMENT, AND (III) THE TERM **"ORDER FORM"** MEANS AN ORDER FORM SIGNED OR OTHERWISE SUBSCRIBED TO BY AN AUTHORIZED REPRESENTATIVE OF CUSTOMER THAT SPECIFIES THE PRODUCTS AND SERVICES TO BE PROVIDED HEREUNDER, THE FEES ASSOCIATED THEREWITH AND ANY OTHER APPLICABLE TERMS AND HAS BEEN ACCEPTED BY PROVIDER, AND SHALL INCLUDE ANY MODIFICATIONS, ADDENDA AND SUPPLEMENTS TO SUCH ORDER FORM. WHEN USED IN THIS AGREEMENT, CAPITALIZED TERMS THAT ARE DEFINED IN SECTION 20 BELOW SHALL HAVE THE RESPECTIVE MEANINGS ASCRIBED TO THOSE TERMS IN SECTION 20. ALL OTHER CAPITALIZED TERMS USED IN THIS AGREEMENT HAVE THE RESPECTIVE MEANINGS ASCRIBED TO THEM IN THIS AGREEMENT.

CUSTOMER MAY ACCEPT THIS AGREEMENT EITHER BY (1) CLICKING A BOX INDICATING ACCEPTANCE, OR (2) EXECUTING AN ORDER FORM THAT REFERENCES THIS AGREEMENT, WHICHEVER OCCURS FIRST. BY ACCEPTING THIS AGREEMENT, CUSTOMER AGREES TO THE TERMS OF THIS AGREEMENT. IF THE INDIVIDUAL ACCEPTING THIS AGREEMENT IS ACCEPTING ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, SUCH INDIVIDUAL REPRESENTS THAT THEY HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THIS AGREEMENT, IN WHICH CASE THE TERM "CUSTOMER" SHALL REFER TO SUCH ENTITY CONSISTENT WITH THE PREVIOUS PARAGRAPH. IF THE INDIVIDUAL ACCEPTING THIS AGREEMENT DOES NOT HAVE SUCH AUTHORITY, OR DOES NOT AGREE WITH THE TERMS AND CONDITIONS OF THIS AGREEMENT, SUCH INDIVIDUAL MUST NOT ACCEPT THIS AGREEMENT AND MAY NOT USE THE PRODUCTS OR SERVICES.

THIS AGREEMENT IS EFFECTIVE BETWEEN CUSTOMER AND PROVIDER AS OF THE DATE OF CUSTOMER'S ACCEPTANCE OF THIS AGREEMENT (THE "**EFFECTIVE DATE**").

1. The Products and Services

(a) Provision of Work. This Agreement governs Customer's (i) subscription to and use of one or more products that are ordered by Customer and made available by Provider to Customer (each a "**Product**" and collectively, the "**Products**") and/or, (ii) the provision of professional services provided by Provider or an Affiliate to Customer (the "**Services**"), each as further described in one or more Order Form(s).

(b) The Products and Services. Unless otherwise specified in the applicable Order Form, each Product is purchased as a subscription for the term stated in the applicable Order Form. Customer agrees that Customer's subscription to each Product is not contingent on the delivery of any future functionality or features, or dependent on any oral or written comments made by Provider regarding future functionality or features. Customer further agrees that Customer may purchase Services from Provider or an Affiliate which are related to the purchase of Products, or independent of and unrelated to any Product. All Services, including those related to installation, training, implementation and configuration of the Products, shall be provided under this Agreement and further specified in the appliable Order Form.

2. License Grant and Restrictions

(a) Subscription to the Products. Subject to the terms of this Agreement, Provider hereby grants to Customer a non-sublicensable, non-transferable, non-exclusive subscription license for Customer's use of the Products by the quantity of subscription Users as specified in an associated Order Form, solely for Customer's internal business purposes. User subscription licenses are for designated Users and cannot be shared or used by more than one User but may be reassigned to new Users replacing former Users who no longer require ongoing use of the Product. Provider reserves all rights not expressly granted to Customer in this Agreement.

(b) Additional Users. If Customer wishes to add additional Users ("**Additional Users**") for any Product, Customer must contact Provider and Provider shall make the Product available for the Additional Users on the terms and conditions set forth in this Agreement and the applicable Order Form. With respect to Additional Users: (i) the term access of any Additional Users to any Product will be coterminous with the preexisting Product subscription term (either the initial

subscription term or any renewal subscription term) and all other terms of this Agreement and the applicable Order Form, and (ii) Customer will be responsible for any additional fees for any additional use exceeding the authorized number of Users.

(c) Restrictions. Customer shall not (i) license, sublicense, sell, resell, or otherwise use any Product or Service for a third party's benefit unless expressly authorized in writing by Provider; (ii) transfer, assign, distribute or otherwise commercially exploit or make any Product, the Services, the Asymbl System or any Content available to any third party not authorized by Provider; (iii) modify or make derivative works based upon any of the Products, the Services or the Content; (iv) create internet links to any of the Products or frame or mirror any Content on any other server or wireless or Internet-based device; (v) reverse engineer or decompile any of the Products, the Services or the Asymbl System; (vi) interfere with or misuse any of the Products or the Services in any manner; (vii) upload Customer Data to any of the Products that contains any viruses or programming routines, macros, or other elements that may damage, surreptitiously intercept or expropriate any system, data or personal information; or (viii) access any of the Products for purposes of monitoring its availability, penetration or security testing, or for any benchmarking or competitive purposes.

(d) Customer's Responsibilities. Customer shall: (i) use commercially reasonable efforts to prevent unauthorized access to, or use of, the Products and Services, and notify Provider promptly of any unauthorized use of any password or account or any other known or suspected breach of security; (ii) report to Provider promptly and use reasonable efforts to stop immediately any unauthorized copying or distribution of Content that is known or suspected by Customer or Customer's Users; and (iii) not impersonate another user of any Product or provide false identity information to gain access to or use any of the Products or Services.

(e) Salesforce.com. Provider makes no representations or warranties regarding third party service providers, including but not limited to, Customer's access to Salesforce.com Services. Regardless of Customer's access to or license to Salesforce.com Service or any other third party service, Customer is subject to the terms of this Agreement and Customer's inability to fully access or utilize the Products due to access to Salesforce, Salesforce.com, or a third party service provider is not grounds to terminate this Agreement nor is it a reason for Customer to default on any or all provisions of this Agreement or the licensing fees.

3. Compliance with Laws

(a) Customer is responsible for all activity occurring under Customer's User accounts and shall abide by all applicable local, state, national and foreign laws, treaties and regulations in connection with Customer's use of the Products and Services, including those related to data privacy, international communications and the transmission of technical or personal data.

(b) Provider shall abide by all applicable local, state, national and foreign laws, treaties and regulations in connection with providing the Products and Services, including those related to data privacy, international communications, and the transmission of technical or personal data.

4. Support, Service Level and Security

(a) Provider will provide the support and service levels for the Products as set forth in Exhibit A, attached hereto and incorporated by this reference (the "**Service Level Agreements**").

(b) Provider has implemented and will maintain Appropriate Security Measures based upon industry best practices. Provider may update these security procedures from time to time but will not materially reduce their scope during the term of this Agreement.

(c) Customer acknowledges and agrees that Provider will use its commercially reasonable efforts to maintain Customer's access to and use of the Products, but such access and use is dependent upon and subject to the availability of the Salesforce.com Service.

5. Intellectual Property Ownership

(a) Provider Intellectual Property. Provider owns all rights, title and interest, including all related Intellectual Property Rights, in and to the Asymbl System, the Products, the Services, the Content, and all improvements, enhancements, modifications, and derivative works of or included in the foregoing, including any software, applications, inventions or other technology developed in connection with and all intellectual property and proprietary rights in or related to any of the foregoing ("**Provider IP**"). To the extent Customer acquires any right, title or interest in any of the Provider IP, Customer hereby assigns all of its right, title and interest in such Provider IP to Provider.

(b) Customer Intellectual Property. All Intellectual Property Rights in and to the Deliverables, excluding any Provider IP, that are specifically prepared by or on behalf of Provider in the course of performing the Services, that are delivered to Customer and paid for by Customer pursuant to an Order Form shall be the exclusive property of Customer (the "**Customer Intellectual Property**"). Customer hereby grants Provider a non-exclusive, worldwide, sublicensable, perpetual, paid-up right and license to use the Customer Intellectual Property to provide, maintain, protect, and improve the Products and Services and to develop other products and services.

(c) Provider Marks. The Asymbl, Asymbl ATS and Asymbl Time names, the Provider logo, and any other names and logos

associated with the Products and/or Services are trademarks of Provider.

(d) Customer Data. Customer retains all right, title and interest in and to Customer Data. Customer grants to Provider a non-exclusive, royalty-free, worldwide license to reproduce, distribute, modify, and otherwise use and display Customer Data in an aggregated and anonymized manner, including to compile statistical and performance information related to the provision, operation, support, improvement, and development of the Products and Services. Provider will not use or access any Customer Data except as set forth in this Agreement.

(e) Feedback. If Customer or any User provides any feedback to Provider regarding the Provider IP or otherwise, suggesting or recommending any changes, including without limitation, new features, enhancements, or functionality relating thereto, or any comments, questions, suggestions, or other feedback ("**Feedback**"), Provider is free to use such Feedback irrespective of any other obligation or limitation between the Parties governing such Feedback. Customer grants Provider a worldwide, perpetual, irrevocable, royalty-free license to use and incorporate into the Provider IP any Feedback provided on or behalf of Customer, and Provider is free to use, without any attribution or compensation to any party, any ideas, know-how, concepts, techniques, or other Intellectual Property Rights contained in the Feedback, for any purpose whatsoever. Notwithstanding the above, Provider is not required to use any Feedback.

(f) No Other Rights. Except as expressly set forth herein, no rights or licenses are granted.

6. Fees and Billing

(a) Fees. Customer will pay all fees for the Products and Services (the "**Fees**") as specified in the associated Order Form(s). Fees for renewal subscription terms for Products will be based on Provider's then-current Fees, unless otherwise stated in an Order Form. The Fees are exclusive of all value added taxes (VAT), other sales tax, any country specific custom duty, licenses, permits, tariffs or import tax (which shall be paid by Customer in addition to the Fees), excluding only United States (federal or state) taxes based solely on Provider's income.

(b) Billing and Payment. Provider issues invoices for each Product on or about the Product subscription start date for the initial subscription term and each renewal date for any renewal subscription term. Fees for Products shall be paid in advance for the period specified on the Order Form or for a period of one (1) year in the case of any renewal subscription term. Fees for Services shall be paid in accordance with the terms of the applicable Order Form. Unless otherwise stated on an Order Form, Fees are due net thirty (30) days from the date of the invoice. For any payment that is past due, Provider may, in its discretion and in addition to any other rights and remedies, impose and require Customer to pay late payment charge(s), upon demand at the lesser of fifteen percent (15%) per month or the highest rate permitted by applicable law. Late charges are calculated from the payment due date until the account is paid and shall be added to the subsequent invoice. All Fees due and payable under an Order Form shall be made to Provider in the currency listed in the Order Form, and in accordance with the instructions on such invoices. Customer is responsible for providing complete and accurate billing and contact information and notifying Provider of any changes to such information. All payment obligations are non-cancelable, and all amounts paid are nonrefundable, except as expressly set forth in this Agreement. If Customer adds additional Users to any Product or allows use of any Product by more than the paid-for number of Users associated with Customer's subscription, Provider will invoice Customer for the additional applicable fees at the same rate for the current term.

(c) Offset. Customer acknowledges that Provider may, in addition to its other rights and remedies, set off any amount owed to Provider or Provider's Affiliates from Customer under this Agreement, any Order Form, or any other agreement with Provider or Provider's Affiliates against amounts owed by Customer, to Provider or Provider's Affiliates under this Agreement, an Order Form or any other agreement with Provider or Provider's Affiliates. Any and all costs and expenses, and all credits, refunds, and obligations, due to Provider or Provider's Affiliates under this Agreement or an Order Form shall be (i) paid by Customer to Provider; or (ii) offset by Provider or Provider's Affiliates against any of Customer's unpaid invoices, at Provider's option. Payments suspended or offset in good faith by Provider will not be a basis for Customer suspending its own performance under this Agreement or declaring Provider in breach of this Agreement or an Order Form. Customer may not set off any amount due from Provider, whether under this Agreement, an Order Form or otherwise, against any amount due to Provider or due to Provider's Affiliates hereunder without Provider's prior written consent.

7. Term

(a) Term of Agreement. The term of this Agreement commences on the Effective Date and continues until (i) the expiration or termination of all of Customer's Order Forms, or (ii) if earlier, termination of this Agreement pursuant to Section 9(b) below.

(b) Term of Product Subscriptions. The term of each Product subscription shall be as specified in the applicable Order Form. Except as otherwise specified in an Order Form, Product subscriptions will automatically renew for additional one year terms, unless either party gives the other written notice of non-renewal at least thirty (30) days before the end of the relevant Product subscription term. In the case of free trials, notifications provided through the applicable Product indicating the remaining number of days in the free trial shall constitute notice of termination, or the number of days stated on a trial Order Form shall constitute notice of termination. Except as expressly provided in the applicable Order Form, renewal of promotional or one-time priced Product subscriptions will be at Provider's applicable list price

in effect at the time of the applicable renewal. All Product subscriptions shall terminate at the same time as any termination of this Agreement pursuant to Section 9(b) below.

8. Third-Party Products

(a) Third Party Products and Terms. In connection with Customer's license and use of the Products, Customer may elect to purchase one or more Third Party Products. The Third Party Products are subject to their own terms and conditions of service and/or use, including, but not limited to, warranties (if any) and ownership of intellectual property (the "**Third Party Terms**"). Such Third Party Terms and the applicable flow-through provisions are an integral part of this Agreement and Customer's breach of such Third Party Terms shall be deemed a breach of this Agreement. If Customer does not agree to abide by the applicable Third Party Terms, then Customer should not install or use such Third Party Products.

(b) No Representations or Warranties. Customer acknowledges and agrees that the use of the Third Party Products is at Customer's sole risk. THE THIRD PARTY PRODUCTS AND RELATED DOCUMENTATION ARE PROVIDED "AS IS" AND WITHOUT ANY WARRANTY OF ANY KIND AND PROVIDER EXPRESSLY DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES, EXPRESS OR IMPLIED, INCLUDING (WITHOUT LIMITATION) ANY IMPLIED WARRANTIES OF MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE OR USE, INCLUDING CUSTOMER'S PARTICULAR BUSINESS OR INTENDED USE, OR OF THE THIRD PARTY PRODUCT'S RELIABILITY, PERFORMANCE OR CONTINUED AVAILABILITY. PROVIDER HAS NO LABILITY FOR ANY THIRD PARTY PRODUCTS WHICH THE CUSTOMER CHOOSES TO USE, INCLUDING THE THIRD PARTY PRODUCTS INABILITY TO ACCESS CUSTOMER DATA FOR ANY REASON NOT DUE TO PROVIDER.

9. Suspension and Termination

(a) Suspension. If Customer is in breach of this Agreement, an Order Form, or in breach of another agreement with an Provider Affiliate due to non-payment such that payment is due and owing for fifteen (15) calendar days past the due date, in addition to any other rights or remedies, Provider may suspend Customer's and any and all of Customer's User's access to and use of the Products and Services until Customer has cured the breach.

(b) Termination. In addition to Provider's suspension rights, Provider may terminate this Agreement and any Order Form, and all Product subscriptions thereunder, upon written notice to Customer if: (i) Customer breaches this Agreement or an Order Form and does not cure such breach within thirty (30) days after written notice of such breach; (ii) if Customer becomes insolvent, make an assignment for the benefit of creditors, commence any proceedings in bankruptcy or consent to any bankruptcy or similar proceedings; or (iii) Provider determines, in its sole discretion, that such termination is necessary to prevent the unauthorized disclosure of confidential or proprietary information. Upon the expiration or termination of this Agreement for any reason, any amounts which Customer owes to Provider under this Agreement or an Order Form for the period prior to such termination will become immediately due and payable, and Provider will terminate Customer's access to and use of the Products and Services. Sections 5, 6, 9-15 and 17-20 will survive the termination or expiration of this Agreement. In no event will termination relieve Customer of Customer's obligation to pay any Fees payable to Provider for the period prior to the effective date of termination.

10. Representations and Warranties

(a) Mutual Warranty. Each party represents and warrants that it has the legal power and authority to enter into this Agreement.

(b) Data Warranty. Customer represents and warrants that Customer owns or has obtained all rights, consents, permissions, or licenses necessary to allow the Products to access, possess, manipulate, process, or use Customer Data and User Details.

11. Disclaimer of Warranties

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, PROVIDER MAKES NO WARRANTIES, REPRESENTATIONS OR GUARANTIES OF ANY KIND, AND ALL CONTENT IS PROVIDED TO CUSTOMER STRICTLY ON AN "AS-IS, AS-AVAILABLE" BASIS. PROVIDER HEREBY DISCLAIMS, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAWS, ALL OTHER IMPLIED OR STATUTORY WARRANTIES, REPRESENTATIONS AND GUARANTIES OF EVERY NATURE AND KIND WHATSOEVER, EXPRESS OR IMPLIED BY LAW, INCLUDING ANY STATUTE OR REGULATION, OR ARISING FROM CUSTOM OR TRADE USAGE OR FROM ANY COURSE OF DEALING OR PERFORMANCE, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, TITLE, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

12. Mutual Indemnification

(a) Customer's Indemnity. Customer shall indemnify and hold Provider and its affiliates, officers, directors, employees, and agents harmless from and against any and all claims, costs, damages, losses, liabilities and expenses (including reasonable attorneys' fees and costs) arising out of, or in connection with (i) a breach of this Agreement or an Order Form by Customer, Customer's employees or agents, (ii) the negligent or unlawful use of the Products or Services or any aspect thereof by Customer, Customer's employees or agents, or (iii) a third party infringement or similar claim due to the Services, Asymbl System's or any Products access to, possession of, manipulation of, processing of, or use of, the Customer Data or User Details as is necessary to provide the Products or Services.

(b) Provider's Indemnity. If any action is instituted by an unaffiliated third party against Customer based upon a claim that the Products or Services, as provided to Customer, infringe a copyright, registered patent or trademark, then Provider shall indemnify, defend and hold Customer and Customer's affiliates, officers, directors, employees, and agents

harmless from and against the claims, costs, damages, and expenses (including reasonable attorneys' fees and costs) arising out of, or in connection with such claim brought by an unaffiliated third party as are finally awarded against Customer or paid in settlement of such claim. Provider also may, at its option and expense: (i) procure for Customer the right to continue using the Products and Services, (ii) replace or modify the Products and Services so that it is no longer infringing but continues to provide comparable functionality, or (iii) terminate this Agreement and the applicable Order Form and Customer's access to the Products and Services and refund any amounts previously paid for the Products and Services attributable to the remainder of the then-current subscription term(s). Provider will have no liability to Customer for any infringement action that arises out of a breach of the terms and conditions of this Agreement by Customer or of the use of the Products or Services (Y) after any Product or Service has been modified by Customer or a third party without Provider's prior written consent, or (Z) in combination with any other service, equipment, software or process not provided by Provider where the combination is the basis for the infringing activity. THIS SECTION SETS FORTH THE ENTIRE OBLIGATION OF PROVIDER AND CUSTOMER'S EXCLUSIVE REMEDY AGAINST PROVIDER OR ANY OF ITS AFFILIATES OR SUPPLIERS FOR ANY INFRINGEMENT CLAIM.

(c) Procedure. A party seeking indemnification under this Section 12 will: (i) give written notice of the claim promptly to the other party, (ii) give the other party sole control of the defense and settlement of the claim, and (iii) provide to the other party all available information and assistance.

13. Insurance; Limitations of Liability

(a) Insurance. During the term of this Agreement, Provider will, at its cost, maintain (i) workers' compensation and technology errors and omissions insurance policies, and (ii) any other insurance required by law in any jurisdiction where Provider provides Services under this Agreement. During the term of this Agreement, Customer will, at Customer's cost, maintain all insurance required by law in any jurisdiction where Customer operates Customer's business and/or uses the Products or Services. All policies required under this Section will be written by reputable national insurance carriers.

(b) LIMITATION OF LIABILITY. PROVIDER'S AGGREGATE LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT WILL IN NO EVENT EXCEED THE AMOUNT PAID BY CUSTOMER HEREUNDER IN THE TWELVE (12) MONTHS PRECEDING THE ACT, OMISSION, ERROR OR BREACH GIVING RISE TO SUCH LIABILITY. THE ABOVE LIMITATIONS WILL APPLY WHETHER AN ACTION IS IN CONTRACT OR TORT AND REGARDLESS OF THE THEORY OF LIABILITY. HOWEVER, THE ABOVE LIMITATIONS WILL NOT LIMIT CUSTOMER'S PAYMENT OBLIGATIONS UNDER SECTION 6. IN NO EVENT MAY A CAUSE OF ACTION BE ASSERTED AGAINST PROVIDER UNDER THIS AGREEMENT WHICH ARISES OUT OF OR RELATES TO ANY EVENT OCCURRING MORE THAN ONE (1) YEAR PRIOR TO THE FILING OF SUCH CAUSE OF ACTION.

(c) NO SPECIAL DAMAGES. IN NO EVENT SHALL PROVIDER OR ANY PROVIDER AFFILIATE BE LIABLE TO ANYONE FOR ANY INDIRECT, PUNITIVE, SPECIAL, EXEMPLARY, INCIDENTAL, CONSEQUENTIAL OR OTHER SPECIAL DAMAGES OF ANY TYPE OR KIND (INCLUDING LOSS OF REVENUE, PROFITS, DATA, USE OR OTHER ECONOMIC ADVANTAGE) ARISING OUT OF, OR IN ANY WAY CONNECTED WITH THE PRODUCTS, THE THIRD PARTY PRODUCTS, OR SERVICES, AN ORDER FORM OR THIS AGREEMENT, EVEN IF PROVIDER HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, TO THE MAXIMUM EXTENT ALLOWABLE BY APPLICABLE LAW.

14. Confidentiality.

(a) Confidential Information. Each party (the **"Disclosing Party"**) may from time to time disclose to the other party (the **"Receiving Party"**) certain information regarding the business, products, or services of the Disclosing Party and its suppliers, including technical, marketing, financial, employee, planning, Customer Data, User Details, and other confidential or proprietary information, including information that the Receiving Party knew or should have known, under the circumstances, was considered confidential or proprietary by the Disclosing Party (**"Confidential Information"**).

(b) Protection of Confidential Information. The Receiving Party will not use any Confidential Information of the Disclosing Party for any purpose other than exercising its rights or exercising its obligations under this Agreement, and will disclose the Confidential Information of the Disclosing Party only to the employees or contractors of the Receiving Party who have a need to know such Confidential Information for purposes of this Agreement and who are under a duty of confidentiality no less restrictive than the Receiving Party's duty under this Section 14(b). The Receiving Party will protect the Disclosing Party's Confidential Information from unauthorized use, access, or disclosure in the same manner as the Receiving Party protects its own confidential or proprietary information of a similar nature and with no less than reasonable care.

(c) Exceptions. The Receiving Party's obligations under Section 14(b) with respect to any Confidential Information of the Disclosing Party will not apply if such information: (i) was already known to the Receiving Party without restriction at the time of disclosure by the Disclosing Party; (ii) was disclosed to the Receiving Party by a third party who had the right to make such disclosure without any confidentiality restrictions; (iii) is, or through no fault of the Receiving Party has become, generally available to the public; or (iv) was independently developed by the Receiving Party without access to or use of the Disclosing Party's Confidential Information. In addition, the Receiving Party will be allowed to disclose Confidential Information of the Disclosing Party to the extent that such disclosure is (x) approved in writing by the Disclosing Party; (y) necessary for the Receiving Party to enforce its rights under this Agreement in connection with a legal proceeding; or (z) required by law or by the order of a court of similar judicial or administrative body, provided that the Receiving Party notifies the Disclosing Party of such required disclosure promptly and in writing and

cooperates with the Disclosing Party, at the Disclosing Party's request and expense, in any lawful action to contest or limit the scope of such required disclosure. Disclosure pursuant to clause (z) of the preceding sentence shall not render Confidential Information as non-confidential or remove such Confidential Information from the obligations of the confidentiality obligations set forth in this Section 14.

(d) Return of Confidential Information. Upon the expiration or termination of this Agreement, and following a written request from the Disclosing Party, the Receiving Party will return to the Disclosing Party or use reasonable efforts to destroy all Confidential Information of the Disclosing Party in the Receiving Party's possession or control. Upon request, the Receiving Party will certify in writing signed by an officer of the Receiving Party that it has fully complied with its obligations under this Section 14(d). Notwithstanding the foregoing, the Receiving Party may retain a limited number of electronic backup copies of Confidential Information as are automatically created and retained by the Receiving Party's standard backup processes and systems. The Receiving Party shall comply with its nondisclosure obligations under this Agreement with regard to such copies and shall destroy them in accordance with Receiving Party's normal destruction processes.

(e) Injunctive Relief. Each party acknowledges and agrees that, in the event of a breach or threatened breach of this Section 14, damages will not be an adequate remedy and accordingly, the Disclosing Party may be entitled to seek injunctive relief against such breach or threatened breach in addition to any other remedies available to such party.

15. Compliance and Privacy

(a) Export and Anti-Corruption. The Products, Services, the Content, and other technology Provider makes available to Customer, and any derivatives thereof, may be subject to export laws and regulations of the United States and other jurisdictions. Each party represents that it is not named on any U.S. government denied-party list. Customer shall not permit Users to access or use the Products, Services or Content in a U.S.-embargoed country or in violation of any U.S. export law or regulation. Customer has not received or been offered any illegal or improper bribe, kickback, payment, gift, or thing of value from any of Provider's employees or agents in connection with this Agreement. Reasonable gifts and entertainment provided in the ordinary course of business do not violate the above restriction. If Customer learns of any violation of the above restriction, Customer will use its best efforts to promptly notify Provider at legal@asymbl.com.

(b) Data Security and Privacy. Because the provision of the Products and/or may require Provider to receive, store, transmit or manage Customer Data, Provider and Customer hereby agree to comply with the provisions of Exhibit B, attached hereto, and otherwise will ensure appropriate protection and handling of Customer Data.

16. Assignment; Binding Effect

Neither this Agreement nor any rights or obligations hereunder may be assigned or transferred by Customer without the prior written consent of Provider. Any attempted assignment or transfer in violation of the foregoing will be void. This Agreement shall be binding on and inure to the benefit of the parties hereto and their respective heirs, representatives, successors and permitted assigns. Any purported assignment in violation of this Section shall be null and void and have no effect.

17. Notices

All notices required or permitted under this Agreement must be delivered in writing by courier, email or by certified or registered mail (postage prepaid and return receipt requested) to the other party. Notices hereunder will be effective (a) upon receipt or 3 days after being deposited in the U.S. Mail as required above, whichever occurs sooner, or (b) if delivered by email, upon confirmation by the receiving party of receipt of the particular email. Any notice to Provider must be delivered to Asymbl, Inc., 3005 S. Lamar Blvd, Ste D109 #369, Austin, Texas 78704 or to legal@asymbl.com.

18. Governing Law; Venue

This Agreement, and its negotiation, execution, delivery, performance and enforcement, shall be governed by and construed in accordance with the substantive and procedural laws of the State of Texas, without giving effect to any conflicts of laws principles that require the application of the law of a different jurisdiction. Any disputes, actions, claims or causes of action arising out of or in connection with this Agreement, the Products, or the Services shall be subject to the exclusive jurisdiction of the state and federal courts located in Austin, Texas.

19. General

If any legal action or other proceeding is brought in connection with this Agreement, the prevailing party shall be entitled to recover reasonable attorneys' fees and costs, in addition to any other relief to which such party may be entitled. If any provision of this Agreement is held by a court of competent jurisdiction to be invalid or unenforceable, then such provision shall be construed, as nearly as possible, to reflect the intentions of the invalid or unenforceable provision, with all other provisions remaining in full force and effect. The parties are independent contractors and this Agreement does not create any joint venture, partnership, employment, or agency relationship between them. The failure of either party to enforce any right or provision in this Agreement shall not constitute a waiver of that or any future right or provision. The descriptive headings of the sections, and subsections of this Agreement are for convenience of reference only. They do not constitute a part of this Agreement and do not affect this Agreement's construction or interpretation. This Agreement, together with any associated Order Form, comprises the entire agreement between Customer and Provider and supersedes all prior or contemporaneous negotiations, discussions or agreements, whether written or oral, between the parties regarding the subject matter contained herein, including any previously executed electronic version

of an Provider subscription or service agreement, commonly known as a clickthrough or end user license agreement. In the event of a conflict between the terms in this Agreement and the terms in any Order Form, the Order Form will control. Any delay in or failure of performance by either party under this Agreement will not be considered a breach of this Agreement to the extent caused by any Force Majeure Event.

20. Definitions

As used in this Agreement the following terms have these meanings:

(a) **"Appropriate Security Measures"** means commercially reasonable technical, physical, and procedural controls to (i) protect Customer Data and User Details against destruction, loss, alteration, unauthorized disclosure to third parties, and unauthorized access by employees or contractors employed by Provider, and (ii) prevent the introduction of any malicious code, files, scripts, agents or programs intended to do harm, including without limitation, viruses, worms, time bombs and Trojan horses, into the Products and the Content.

(b) **"Asymbl System"** means the hardware, software, network equipment, and other technology used by Provider to deliver the Products, and any other of Provider's proprietary technology (including software, hardware, products, processes, algorithms, user interfaces, know-how, techniques, designs and other tangible or intangible technical material or information) made available to Customer by Provider in providing the Products.

(c) **"Content"** means the visual information, documents, software, products and services contained or made available to Customer in the course of using the Products and Services, other than the Products and Services themselves, Customer Data and User Details.

(d) **"Customer Data"** means any information (including without limitation personally identifiable information) provided, made available, or submitted by Customer to any of the Products or retrieved by any of the Products from another source as directed by Customer other than User Details.

(e) "**Deliverables**" means the output provided as part of the Services or as otherwise described in an Order Form.

(f) **"Force Majeure Event"** means events or circumstances beyond a party's reasonable control, including without limitation, acts of God, acts of government, flood, fire, earthquakes, civil unrest, acts of terror, pandemics, epidemics, strikes or other labor problems, telecommunications or network failures or delays, service or computer failures involving services, hardware, or software not within Provider's possession or reasonable control, and acts of vandalism, including network intrusions and denial of service attacks. For the avoidance of doubt, Customer acknowledges that Customer's inability to pay the Fees or to access the Salesforce Service is not a Force Majeure Event and Customer expressly assumes such risk that its ability to utilize the Products can be impaired by its inability to use or access Salesforce.com Services. Customer's payment obligations under this Agreement shall remain in effect regardless of any Force Majeure Event.

(g) "**GDPR**" means the General Data Protection Regulation of the European Union.

(h) **"Intellectual Property Rights"** means unpatented inventions, patent applications, patents, design rights, copyrights, trademarks, service marks, trade names, domain name rights, mask work rights, know-how and other trade secret rights, and all other intellectual property rights, derivatives thereof, and forms of protection of a similar nature anywhere in the world.

(i) **"Salesforce.com Service"** means the service provided by salesforce.com to which Customer must be a subscriber in order to obtain the Products.

(j) "**Third Party Products**" means application software products provided by third party vendors, including operating system and application software with which the Software may interface.

(k) "**Third Party Vendors**" means the manufacturers, authors, developers, vendors, and/or service providers of the Third Party Products.

(l) **"User(s)"** means Customer's named employees, representatives, consultants, contractors, partners, or agents who are authorized to use the Products by Customer through the Salesforce LMA (License Management Application) or the user management facility of the Products.

(m) **"User Details"** means basic information collected by Provider about Customer's Users authorized by Customer to use the Products which is used for subscription management, activity logging, communications to Users by Provider, and technical support purposes.

Exhibit A

Service Level Agreement

This Service Level Agreement details Provider's commitments in relation to availability and performance of the Products, related support services and problem resolution.

1. Definitions.

(a) **"Business Hours"** shall mean 3 a.m. to 6 p.m. Central Standard Time, Monday through Friday, except for national holidays.

(b) **"Excluded Downtime"** means any time the Products are not available because of a Force Majeure Event, Planned Downtime, or unavailability of the Salesforce.com Service.

(c) **"Paid Support"** means Providers provision of support services to Customer as stated in an associated Order Form.

(d) **"Planned Downtime"** means any period of time during which the Product are unavailable due to Provider's planned maintenance and support of the Products or the Asymbl System. Planned Downtime shall not exceed five (5) hours per month. Provider will endeavor to give at least twenty-four (24) hours' notice before Planned Downtime except for urgent circumstances (e.g., a system failure or security threat).

(e) **"Service Level Incident"** means a reproducible non-conformity in the Products causing the Products to not operate in substantial conformance with the product description(s) supplied by Provider from time to time.

(f) **"Support Services"** means technical support assistance, including Basic Support and Paid Support, provided by Provider personnel to Customer's designated administrators for problem resolution, bug reporting, and technical assistance, which, in each case, is related to a Service Level Incident.

(g) **"Total Minutes"** means the total number of minutes in the calendar month at issue.

(h) **"Unplanned Downtime"** means any time (i) the Products are not available because of an event or circumstance other than Planned Downtime, and (ii) the amount of time required by Provider to resolve or provide a work-around for the failure of any documented feature required to complete a primary function of the Products.

2. Service Availability and Performance.

The Service Availability "Uptime" will generally be equal to or greater than 99.7% in each calendar month and the Products will perform in substantial conformance with the product description(s) supplied by Provider from time to time except for Excluded Downtime, where "**Uptime**" = (Total Minutes - Unplanned Downtime - Excluded Downtime) / (Total Minutes - Excluded Downtime) X 100.

3. Support Services and Problem Resolution.

Customers' provisions of the Products shall include a total of two (2) hours of live support for the subscription term (such support "**Basic Support**"). Basic Support will be based on this Exhibit A. Customer may elect to purchase additional Support Services from Provider (such additional support, "**Paid Support**"). If Customer purchases Paid Support from Provider, the fees for such Paid Support shall be further provided in an associated Order Form and shall be for the current subscription term. Support Services for Paid Support shall be provided by Provider to Customer in accordance with the procedures and within the time periods set forth in Annex 1 attached hereto to Exhibit A.

Customer receiving Support Services from Provider is subject to Customer paying all applicable Fees due and owing to Provider. Support Services will be provided to Customer's administrator(s) during Business Hours in the English language. To receive Support Services, Customer must submit a case at support@asymbl.com.

Annex 1 to Exhibit A

Problem Response and Resolution

Provider will address Service Level Incidents in accordance with the terms below.

Problem Severity Level	Response Time	Resolution Time
Level 1: The Products are not available for use, including the failure of a critical feature of the Products.	Provider's support team will respond within 4 Business Hours. Provider's technical team will commence efforts to address Level 1 problems within 1 hour after Customer's report of such problem is received by Provider or Provider's detection of such problem, whichever is earlier.	Provider will use commercially reasonable efforts, 24 hours per day, 7 days per week, to resolve or provide Customer with an acceptable work-around for the applicable Level 1 problem. Provider will keep Customer updated regularly on the progress of the resolution.
Level 2: A documented feature is not available but does not prevent the use of a critical feature of the Products.	Provider's support team will respond within 8 Business Hours. Provider's technical team will commence efforts to address Level 2 problems within 8 Business Hours after Customer reports such problem during Business Hours or Provider's detection of such problem, whichever is earlier.	Provider will use commercially reasonable efforts, during normal Business Hours, to resolve or provide Customer with an acceptable solution for the Level 2 problem within 5 business days after Customer reports such problem or Provider's detection of such problem, whichever is earlier.
Level 3: A documented feature is impaired but does not prevent the use of a critical feature of the Products.	Provider's support team will respond within 16 Business Hours. Provider's technical team will commence efforts to address Level 3 problems within 3 business days after Customer reports such problem during Business Hours or Provider's detection of such problem, whichever is earlier.	Provider will use commercially reasonable efforts, during normal Business Hours, to resolve or provide Customer with an acceptable solution for the Level 3 problem within 60 calendar days after Customer reports such problem or Provider's detection of such problem, whichever is earlier.
Level 4: A Level 4 issue is a general usage question or issue that may be cosmetic in nature or documentation related. Provider software works without any functional limitation.	Provider's support team will respond within 16 Business Hours.	
Enhancement Request ("**ER**"): An enhancement request is a request for future product enhancement or modification to add official support and documentation for unsupported, undocumented, or features that do not exist in the Provider software.	Provider's support team will respond within 16 Business Hours. Response is limited to a support representative triaging the request to provide feedback about possible workarounds and confirmation the enhancement request has been created.	Provider will take ERs into consideration in the product management process but has no obligation to deliver enhancements based on any ER.

Customer acknowledges that the Products are dependent on Customer's implementation and configuration of the Products and the availability and performance of technology from third-party software and hardware vendors including but not limited to salesforce.com, Salesforce AppExchange products and custom applications, Microsoft, Google, and the providers of Internet browsers. Provider has no control over, and is not liable for, performance issues or downtime of the Products to the extent caused by such factors.

Encryption gateways and associated third party technology that require any re-direction of Asymbl-to-Salesforce connections are not eligible for Support Services. Customer may utilize such encryption solutions solely at Customer's own risk.

EXHIBIT B
DATA PROCESSING ADDENDUM

This Data Processing Addendum (the "**DPA**" or "**Addendum**") is incorporated into and forms part of the Master Services Agreement between Customer and Provider to which this DPA is attached (the "**Agreement**"). In the event of a conflict between the DPA and Agreement, the terms and conditions of this DPA will prevail.

1. **Definitions**
   Terms defined in the Agreement will, unless otherwise defined in this DPA, have the same meanings when used in this DPA. Further, the following capitalized terms used in this DPA will be defined as follows:

   a. "**Controller**" means the Customer when, alone or jointly with others, it determines the purpose and means of processing Personal Data.

   b. "**Customer Account Data**" means Personal Data that relates to Customer's relationship with Provider, including the names and contact information of the individuals authorized by Customer to access Customer's account and billing information of individuals that Customer has associated with its Account. Customer Account Data also includes any data Provider may need to collect for the purpose of identity verification (e.g., providing multi-factor authentication services) or as part of its legal obligations to maintain records.

   c. "**Customer Data**" means any Customer-provided, non-public or proprietary information exchanged as a result of using the Service form, including Customer Personal Data.

   d. **"Customer Personal Data**" means any Personal Data processed by Provider on behalf of Customer in connection with the Services, as furthered described in Schedule 1. Customer Personal Data includes the Personal Data of Customer's third parties for whom Customer acts as a processor.

   e. "**Data Protection Law**" refers to all laws and regulations applicable to Provider's processing of Personal Data under the Agreement.

   f. "**Data Subject**" means a natural person who can be identified, directly or indirectly.

   g. **"Personal Data**" means any information relating to a natural person who can be identified, directly or indirectly.

   h. "**process**" or "**processing**" means any operation or set of operations which is performed upon Customer Data whether or not by automated means.

   i. "**Processor**" means Provider when Provider processes Personal Data on behalf of Customer.

   j. "**Security Breach**" means a breach of Provider's security resulting in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data.

   k. "**Services**" has the same meaning as defined in the Agreement, or if not defined in the Agreement, the processing of Customer Data by Provider on behalf of the Customer described in the Agreement.

   l. **"Subprocessor"** means a processor appointed by Provider to process Customer Personal Data.

2. **Instructions for Data Processing**

   a. *Generally*. The Agreement and this DPA will be the Customer's instructions to Provider for the processing of Customer Data. Provider will process Customer Data solely for the purpose of providing the Services and will ensure that all individuals with access to Customer Data have a duty of confidentiality with respect to that Customer Data. Provider will not sell, share, disclose, retain, or otherwise use Customer Data for any other purpose unless specifically instructed by Customer in writing or as required by law.

   b. *Regulatory and Legal Compliance*. Provider will process Customer Data in compliance with Data Protection Law. Provider will provide reasonable assistance to Customer in complying with its obligations under Data Protection Law. Unless prohibited by law, Provider will notify Customer promptly of any inquiries or complaints received about the processing of Customer Personal Data from regulators or law enforcement authorities. Provider will not respond to any such inquiries or complaints except on the documented instructions of Customer or as required by law. If disclosure of Customer Data is required by applicable law or a compulsory legal process, Provider will, unless prohibited by applicable law: (i) notify Customer promptly in writing before complying with any such disclosure request and provide Customer an opportunity to intervene, if appropriate; and (ii) disclose only the minimum amount of Customer Data necessary to comply with applicable law or a compulsory legal process.

   c. *Data Subject Rights.* Unless prohibited by law, Provider will promptly notify Customer of any request from a data subject with respect to Customer Personal Data. Provider will not respond to any data subject request without Customer's prior written consent, except to confirm that the request relates to Customer. Provider will provide reasonable and timely assistance to Customer in complying with its data protection obligations with respect to data subject rights under Data Protection Law.

   d. *Additional Costs*. If any of the Customer's instructions require processing Customer Data in a manner that falls outside the scope of the Services, Provider may either (a) make the performance of any such instructions subject

to the payment by Customer of any costs and expenses incurred by Provider or such additional charges as Provider may reasonably determine; or (b) terminate the Agreement and the Services.

e. *California Consumer Privacy Act.* To the extent that Customer Data comprises Personal Data (pursuant to the California Consumer Privacy Act "**CCPA**")), it is hereby acknowledged that Provider is acting as a "Service Provider" (pursuant to CCPA) on behalf of Customer. Provider shall: (i) process the Customer Data that is Personal Data only on Customer's instructions (including in accordance with the Agreement and this DPA), (ii) take appropriate technical, organizational and security measures against unauthorized access to or unauthorized alteration, disclosure, destruction or loss of such Personal Data, (iii) take reasonable steps to ensure that employees and/or subprocessors used by Provider to provide the Services are aware of and are suitably instructed in such technical, organizational and security measures, (iv) unless prevented by Data Protection Law, promptly refer to Customer any requests, notices or other communication from Data Subjects or a regulator (such as a data protection authority), and (v) not "sell" any Personal Data, as that term, and its cognates, are defined under the CCPA.

3. Customer Warranties and Undertakings

Customer warrants that it (a) has provided all applicable notices and obtained all required consents required for the lawful processing of Customer Data; and (b) has reviewed the security measures set out in Schedule 3 and agrees that the security measures are appropriate based on the nature and sensitivity of the Customer Data.

4. Subprocessors

a. *Conditional Authorization.* Customer provides a general authorization for Provider to engage downstream Subprocessors that is conditioned on the following requirements:

(i) Provider will impose contractual data protection obligations on any Subprocessor it appoints to process Customer Data to meet the standards required by Data Protection Law and this DPA; and

(ii) Provider will remain liable for any breach of this Addendum that is caused by an act, error, or omission of its Subprocessors.

b. *Current Subprocessors and Notification of Changes*. Customer authorizes Provider to engage the Subprocessors listed in Schedule 2 to process Customer Data. Provider may update Schedule 2 by posting a new version of the Subprocessor list at the Asymbl Support Portal or providing Customer 14 days' prior written notice of such change. Customer may object to Provider's appointment or replacement of a Subprocessor prior to its appointment or replacement, provided such objection is in writing and based on reasonable grounds relating to data protection. In such an event, the parties agree to discuss commercially reasonable alternative solutions in good faith. If it can be reasonably demonstrated to Provider that the new Subprocessor is unable to process Customer Personal Data in compliance with the terms of this DPA and Provider cannot provide an alternative Subprocessor, or the parties cannot reach a resolution within 90 days from the date of Provider's receipt of Customer's written objection, Customer may discontinue the use of the affected Services with respect only to those aspects of such Services which cannot be provided by Provider without the use of the new Subprocessor by providing written notice to Provider. Such discontinuation will be without prejudice to any fees incurred by Customer prior to the discontinuation of the affected Services. If no objection has been raised prior to Provider replacing or appointing a new Subprocessor, Customer will be deemed to have authorized the new Sub-processor. Provider may replace a Subprocessor at any time if the need for replacement is urgent and required for reasons beyond Provider's reasonable control, and Provider will notify Customer of the replacement Subprocessor as soon as reasonably practicable, and Customer shall have the right to object to the replacement Subprocessor pursuant to this Section 4.b.

5. International Provisions

a. *Cross Border Data Transfer Mechanisms for Data Transfers*. To the extent Customer's use of the Services requires the transfer of Personal Data from a jurisdiction identified in Schedule 4 to a location outside of that jurisdiction ("**Transfer Mechanism**"), the terms set forth in Schedule 4 (Cross Border Transfer Mechanisms) of this Addendum will apply.

6. Security Measures and Audits

a. *Security Measures.* Provider will implement reasonable physical, organizational, and technical measures to protect against any unauthorized or unlawful access, processing, loss, destruction, theft, damage, use or disclosure of Customer Data or systems (collectively, "**Appropriate Safeguards**"), including, at a minimum, the security measures set forth as Schedule 3. These Appropriate Safeguards will be appropriate to the harm that might result from any risks to Customer Data or systems and having regard to the nature of the Customer Data or system which is to be protected and will take into consideration the state of the art, the costs of implementation and the nature, scope, context and purpose of the processing and the risks to the rights and freedoms of the Personal Data subjects.

b. Variation of Measures. Provider may review and update Schedule 3 from time to time, provided that any such updates shall not materially diminish the overall security of the Service or Customer Personal Data.

c. *Compliance Review.* Provider will cooperate with reasonable assessments by Customer as to its compliance with this DPA and Data Protection Law. Customer may provide a written request Provider to assess Provider's

compliance with the Agreement. Following receipt by Provider of such request, Provider and Customer shall mutually agree in advance of the details of such assessment, including the reasonable start date, scope, and duration of, and security and confidentiality controls applicable to, any such assessment. Any such assessment assessments must be conducted (a) on reasonable written notice to Provider; (b) only during Provider's normal business hours; (c) in a manner that does not disrupt Provider's business; (d) subject to a confidentiality agreement in a form such as Provider may reasonably request; (e) in compliance with relevant policies for individuals visiting Provider's or sub-vendors premises; and (f) at Customer's expense. Provider may charge a fee for any such assessment, provided such rates shall be reasonable, accounting for the resources expended by Provider. Notwithstanding anything to the contrary, the assessment right provided in this Section 6.c may be satisfied by the provision of a successful assessment result performed by an experienced, qualified independent auditor within the last 24 months. Any assessment, assessment result, and any information arising therefrom shall be considered Provider's confidential information and may only be shared with a third party (including a third party controller) with Provider's prior written agreement.

7. Security Breach and Response

a. *Breach Notification.* Provider will promptly notify Customer without undue delay and no later than 72 hours upon Provider becoming aware of a Security Breach. Provider should notify Customer by telephone to Provider's primary business contact and via email to the Customer Data Privacy Contact identified in the Customer profile if it has knowledge that there is an actual or potential Security Breach. To the extent known, notice will include the following: (a) the nature of the Security Breach, (b) the categories and numbers of data subjects concerned, and the categories and numbers of records concerned; (c) the name and contact details from whom more information may be obtained; (d) the likely consequences of the Security Breach; and (e) the measures taken or proposed to be taken to address the Security Breach. The parties acknowledge and agree that Provider is subject to common, unsuccessful attempts to access its systems that do not result in any unauthorized access, use, disclosure, modification, data destruction, or interference with systems operations ("**Unsuccessful Security Incidents**"). Provider hereby notifies Customer of Unsuccessful Security Incidents, including without limitation ping sweeps or other common network reconnaissance techniques, attempts to log onto a system with an invalid password or username, and denial of service attacks that do not result in a server being taken offline, which may occur from time to time, and this sentence shall be deemed to meet the requirements for reporting such Unsuccessful Security Incidents under this Addendum.

b. *Cooperation and Remediation.* Provider will (i) cooperate with Customer in the manner reasonably requested by Customer and in accordance with law to investigate and resolve the Security Breach and to mitigate any harmful effects of the Security Breach; (ii) promptly implement any necessary remedial measures to ensure the protection of Customer Data; and (iii) document responsive actions taken related to any Security Breach.

c. *Information to Third Parties.* Except as required by applicable law or regulation, Provider will not inform any third party of any Security Breach without first obtaining Customer's prior written consent, other than to inform a complainant that Customer will be informed of the Security Breach, and Customer will have the sole right to determine whether notice of the Security Breach is to be provided to any individuals, Supervisory Authorities, regulators, law enforcement agencies, consumer reporting agencies, or others and the contents of any such notice.

8. Liability

Any exclusions or limitations of liability set out in the Agreement will apply to any losses suffered by either party (whether in contract, tort (including negligence) or for restitution, or for breach of statutory duty or misrepresentation or otherwise) under this DPA.

9. Duration and Termination

a. *Return/Deletion of Customer Data.* Provider will, within 30 days of the date of termination or expiry of the Agreement: (a) if requested by Customer within that period, return a complete copy of Customer Data by secure file transfer in such format reasonably agreed to by Provider and Customer; and (b) other than any Customer Data retained by Provider after termination of the Agreement in accordance with the Agreement as expressly permitted by this DPA or as required by the EU Standard Contractual Clauses, delete, and use all reasonable efforts to procure the deletion of all other copies of Customer Data processed by Provider or any sub-processors.

b. *Certification.* Upon Customer's request, Provider will promptly confirm to Customer that it has destroyed or returned all Customer Data. If Provider is unable to return or destroy all Customer Data, Provider will retain Customer Data only to the extent and for such period as required by applicable laws, maintain the security and confidentiality of all such retained Customer Data in accordance with the protections of this DPA, and ensure that such Customer Data is only processed as necessary for the purposes specified in the applicable laws preventing its deletion and for no other purposes.

c. *Compliance with this DPA.* If Provider determines that it can no longer meet its obligations under this DPA or Data Protection Law, Provider will notify Customer of that determination within 5 business days and work with Customer to take reasonable and appropriate steps to stop and remediate the unauthorized use of Customer Data.

10. Law and Jurisdiction

Except to the extent expressly overridden by Schedule 3, the parties agree that the laws, jurisdictions, and venues set forth in the Agreement will also govern this DPA.

11. General

a. *Third Party Rights*. A person who is not a party to this DPA may not enforce any of its terms, except to the extent required by applicable law.

b. *Rights and remedies***.** Except as expressly provided in the Agreement, the rights and remedies provided in this DPA are in addition to, and not exclusive of, any rights or remedies provided by law.

c. *No partnership or agency***.** Nothing in the DPA is intended to, or will be deemed to, establish any partnership or joint venture between any of the parties, constitute any party the agent of another party, or authorize any party to make or enter into any commitments for or on behalf of any other party.

d. *Waiver*. No delay or forbearance by either party in enforcing its rights will prejudice or restrict the rights of that party, and no waiver of any such rights or any breach of any contractual terms will be deemed to be a waiver of any other right or of any later breach.

e. *Severability*. If any provision of the DPA is judged to be illegal or unenforceable, the continuation in full force and effect of the remainder of the provisions of the DPA will not be prejudiced.

SCHEDULE 1 TO DPA
DETAILS OF PROCESSING

1. **Categories of data subjects**

The categories of data subjects whose Personal Data are transferred: (a) employees of Customers who are natural persons, (b) customers or vendors of Customer who are natural persons, (c) employees or contact persons of Customer's third parties and vendors for whom Customer acts as a processor.

2. **Categories of Personal Data**

The transferred categories of Personal Data are: identification and contact information (e.g., *name, address, title, and contact details)* and IT information *(e.g. IP addresses)*.

3. **Special categories of Personal Data (if applicable)**

The transferred Personal Data includes the following special categories of data: Not applicable.

4. **Frequency of the transfer**

The frequency of the transfer is: continuous during the term of the Agreement.

5. **Subject matter / Purpose of the processing**

The subject matter of the processing is: providing Customer with Services as described in the Agreement.

6. **Nature of the processing**

The nature of the processing is: collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, use, transmit or otherwise making available, alignment or combination, restriction, erasure or destruction, in accordance with the Agreement.

7. **Purpose(s) of the data transfer and further processing**

The purpose/s of the data transfer and further processing is/are: to provide and support Customer's use of Provider technology solutions provided under the Agreement.

8. **Duration**

The period for which the Personal Data will be retained, or, if that is not possible, the criteria used to determine that period: as set out in Section 9 of the DPA.

9. **Sub-processor (if applicable)**

See Schedule 2.

SCHEDULE 2 TO DPA
SUBPROCESSORS

Provider (including its affiliates and subsidiaries) may engage and use certain Subprocessors to provide services to its Customers. These Subprocessors may have access to personally identifiable information within the Customer Data provided directly to Provider or the applicable Subprocessor from Customers and their Users or to which Provider may have access to provide the Products and Services or to enable requested features related thereto.

The below table provides information about the identity, location, and role of each Subprocessor who may have access to or process personally identifiable information from or on behalf of Provider.

Provider currently uses the below list of Subprocessors to provide its Products and Services. Not all Subprocessors are used in the provision of all Products and Services provided. Not all Subprocessors are involved in all Products and Services.

Subprocessor	Applicable Products and Services	Nature and Purpose of Processing	Categories of Personal Data	Location of Processing
Cloud Coach	Project Management, Customer Onboarding, Professional Services Automation, Project Portfolio Management, Customer Success	Managing project schedules, resources, collaboration, tracking project time, and managing customer interactions.	Employee and customer contact information, project details, meeting notes, time entries, and stakeholder information.	Primarily on the Salesforce platform, which can vary but often involves data centers in multiple global locations.
Jira	Issue and Project Tracking Software	Tracking issues, bugs, and project tasks; managing workflows; and facilitating team collaboration.	Usernames, emails, project-related communications, and issue details.	Data centers in the US, Germany, Ireland, Singapore, and Australia.
Jenkins	Continuous Integration and Continuous Delivery Automation.	Automating parts of software development related to building, testing, and deploying code.	User credentials, project configuration details, and build logs	Typically hosted on the user's own infrastructure or cloud services chosen by the user.
Git	Version Control System	Managing and tracking changes in source code during software development	Usernames, commit history, and code repositories	User's own infrastructure or hosted Git services (e.g., GitHub, GitLab).
Gearset	Salesforce DevOps	Automating deployment, continuous integration, and backup of Salesforce environments.	Metadata and configuration of Salesforce environments, deployment logs.	Data centers in the US, UK, and Australia.
Trello	Project Management and Collaboration Tool	Managing projects and tasks, facilitating team collaboration.	Usernames, emails, project boards, and card details	US-based data centers
Gurock (TestRail)	Test Case Management	Managing and tracking software testing efforts	Usernames, emails, test case details, and test results	US and Germany
Okta	Identity and Access Management	Managing user identities, authentication, and access to applications.	Usernames, emails, authentication data, and access logs	US, Canada, Europe, and Asia
Drata	Compliance Automation	Automating compliance workflows and monitoring security controls	User credentials, compliance status, and audit logs	US-based data centers.
Gong	Revenue Intelligence Platform.	Analyzing sales calls and interactions to provide insights	Recorded calls, transcripts, and user interactions	US-based data centers.
Ninety.io	Business Operating System	Managing business processes and tracking company performance.	Usernames, emails, meeting notes, and performance metrics.	US-based data centers.
Xink	Email Signature Management.	Managing and standardizing email signatures.	User contact information and email signature details.	US and EU data centers.

Xero	Accounting Software	Managing financial data, invoices, and payroll.	Usernames, financial information, and transaction details.	Data centers in the US and Australia.
Sketch	Design and Prototyping Tool.	Creating and sharing design prototypes and assets.	User credentials and design files.	Primarily US-based data centers.
Salesforce	Customer Relationship Management (CRM) Platform.	Managing customer relationships, sales, and service processes.	Customer contact information, sales data, and service interactions.	Data centers in the US, Europe, and Asia
Miro	Online Collaborative Whiteboard.	Facilitating team collaboration and brainstorming sessions.	Usernames, emails, board content, and comments.	US and Europe.
LucidChart	Diagramming and Visualization Tool	Creating flowcharts, diagrams, and visual representations of data.	User credentials, diagrams, and comments.	US-based data centers
ClickDeploy	Salesforce Deployment Automation.	Automating the deployment of Salesforce changes.	Metadata and configuration of Salesforce environments, deployment logs.	US-based data centers.
Amazon Web Services	Cloud computing services including storage, databases, analytics, networking, mobile, developer tools, management tools, IoT, security, and enterprise applications.	AWS processes data to provide scalable and secure cloud computing services, which include computing power, storage options, and content delivery.	User account details, contact information, payment information, usage data, and service logs.	AWS customers can choose their data processing location from available AWS Regions globally. AWS operates data centers in North America, South America, Europe, Asia, and Australia
Gusto	Payroll, benefits, HR, and compliance management for small to medium-sized businesses.	Processing payroll, managing employee benefits, ensuring tax compliance, and handling other HR tasks.	Employee personal details (name, address, Social Security number), payroll information, benefits data, and tax-related information.	Primarily within the United States.
Keka	HR management, payroll processing, and employee performance management.	Managing HR functions such as attendance, leave, payroll processing, performance reviews, and employee engagement.	Employee personal information, attendance records, payroll details, performance metrics, and feedback data.	Primarily based in India, with data centers possibly located in multiple regions to support global operations.

SCHEDULE 3 TO DPA
TECHNICAL AND ORGANIZATIONAL MEASURES

Description of the technical and organizational security measures implemented by the data importer / Provider to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, as well as the risks for the rights and freedoms of natural persons.

1. **Pseudonymisation and Encryption** *(Art. 32, para 1, point a GDPR)*

a. **Encryption**. Provider encrypts Customer Data at rest using AES 256-bit (or better) encryption. Provider uses encrypted network connections or protocols (e.g., TLS 1.2, HTTPS, VPN) for Customer Data in transit over untrusted networks.

b. **Key Management**. Provider logically separates encryption keys from Customer Data and encryption keys are regularly rotated.

2. **Confidentiality** (*Art 32, para 1, point b GDPR)*

a. **Confidentiality Generally**. Provider uses measures designed to (a) prevent unauthorized persons from gaining access to Provider systems with which Customer Data are stored, processed, or used; (b) prevent systems processing Customer Data from being used without authorization, (c) ensure that persons entitled to use a system that processes Customer Data only have access to the data which they have a right of access, (d) prevent unauthorized reading, copying, modification, or removal of Personal Data in the course of processing or use and after storage, and (e) ensure data collected for different purposes can be processed (stored, amended, deleted, transmitted) separately.

b. **Physical Access Controls**. Provider uses physical access control systems, such as proximity badges, at its offices. Provider requires its Cloud Service Providers meet industry-standard physical security controls, and Provider regularly reviews the appropriateness of such physical controls as audited under the Cloud Service Provider's third-party audits and certifications.

c. **System/Electronic Access Controls**. Provider personnel access Provider systems hosting Customer Data using unique user IDs, multifactor authentication, and passwords in accordance with industry standards. Access to Customer Data is restricted to Provider personnel with a need to access such Customer Data in connection with the Services or as required by law. Provider uses an industry standard security information and event management system. Infrastructure management and configuration management tools are used for security hardening and monitoring baseline configuration standards for Provider systems that process Customer Data.

d. **Isolation/Separation Controls**. Provider allocates permissions and privileges on a least privilege principle and assigns network and data access rights based on user group and job function. Provider regularly reviews Provider personnel's access privileges to Provider systems and removes access on a timely basis for all separated personnel. Provider logically separates Customer Data from its other customers data and logically separates production environments from development environments.

3. **Integrity** *(Art 32, para 1, point b GDPR)*

a. **Encryption**. Provider uses secure transmission between Customer and server and to external systems via industry-standard encryption as set forth in Section 1 of this Schedule.

b. **Firewalls**. Provider maintains firewalls and other measures to appropriately limit access to and from Provider systems. Provider uses industry-standard firewall or security group technologies with deny-all default policies to prevent in-bound and out-bound network protocols to Provider systems other than those that are reasonably required to perform Services in accordance with the Agreement.

c. **Data Input Control**. Provider uses monitoring tools to log certain activities and changes within Provider systems. Provider monitors these logs for abnormalities and securely stores such logs for at least one year.

d. **Anti-Malware**. Provider maintains anti-malware controls to protect against malicious software causing accidental or unauthorized destruction, loss, alteration, disclosure, or access to Customer Data.

4. **Availability and Resilience** *(Art 32 para 1 point c GDPR)*

a. **Backups**. Provider maintains backups of Customer Data stored in the primary Provider system and maintains backups of Customer Data to a secondary system on at least a daily basis.

b. **System Monitoring.** Provider monitors Provider systems using defined processes for security alerting, escalation, and remediation consistent with the applicable Service. Provider uses an issue tracking system to maintain, manage, and track changes to Provider systems. Enterprise monitoring applications are configured to

monitor in-scope systems and alert operation personnel when predefined thresholds are met, and Provider uses tools to monitor security events, latency, and network performance.

c. **Disaster Recovery and Business Continuity Plan**. Provider maintains disaster recovery and business continuity plans designed to minimize interruption of Services. Such plan includes disaster recover incident management, procedures for recovering access to Customer Data, and periodic testing of the disaster recovery plan. Production data centers are designed to mitigate the risk of single points of failure and support service continuity and performance. Incident response procedures that outline security event response are used, and Provider and reviews lessons learned to evaluate effectiveness of the procedures.

5. **Vulnerability Management**.

   a. **Vulnerability Detection**. Vulnerabilities meeting defined risk criteria trigger alerts and are prioritized for remediation based on the potential impact to Services. Provider maintains standard patch management processes for Provider systems to protect against security vulnerabilities.

   b. **Risk Assessments**. Provider performs an annual security operational risk assessment of Provider systems processing Customer Data. Results from risk assessment activities are documented in a risk register and prioritized for treatment by risk level. Provider performs risk-based control monitoring throughout the year by performing control testing using a formal methodology. The testing results are documented and reviewed by management, including remediation plans for identified observations.

6. **Data Governance and Management**.

   a. **Information Security Plan**. Provider maintains a comprehensive, documented information security program designed to protect Customer Data against unauthorized or accidental destruction, loss, alteration, disclosure, or access. Provider maintains commercially reasonable controls for information governance and data management.

   b. **Security Officer**. Provider has appointed one or more security officers to coordinate information security and monitor information security rules and procedures.

7. **Personnel**.

   a. **Roles and Responsibilities**. Provider maintains written policies defining the roles and responsibilities of Provider personnel with access to Customer Data.

   b. **Policies.** Provider requires criminal background screening of Provider employees as part of its hiring process, to the extent permitted by law.

   c. **Confidentiality.** Provider ensures that Provider personnel authorized to access Customer Data are bound to confidentiality obligations or under appropriate statutory obligations of confidentiality.

   d. **Training**. Provider maintains an information security training and awareness program for Provider personnel and requires Provider personnel to complete such training annually.

8. **Data Minimization, Quality, and Portability.**

   a. **Data Minimization, Quality, and Portability**. Provider will use reasonable efforts to use only the minimum necessary Personal Data in the performance of Services. As part of SaaS Services, Customer may access, amend, delete, and extract Customer Data within the applicable SaaS Services to assist Customer with its data quality, minimization, and portability efforts

   b. **Data Destruction.** Provider ensures that residual magnetic, optical, physical, or electrical representations of Personal Data that have been deleted may not be retrieved or reconstructed when storage media is transferred, becomes obsolete, or is no longer usable or required by Provider. Personal Data stored on Provider media (e.g., hard drive, digital media, tapes) must be rendered unreadable using the NIST Guidelines for Media Sanitization prior to the media being disposed of or moved off site.

9. **Testing, Assessing, and Evaluating the Technical and Organization Measures** *(Art. 32 para 1 point D GDPR)*. Provider follows measures to regularly review and assess its technical and organizational measures.

   a. **Internal Assessments**. Provider internal resources review Provider's information security practices on an annual basis.

   b. **Vulnerability Testing**. Provider conducts vulnerability testing on Provider systems in accordance with Section 5 of this Schedule.

   c. **Penetration Testing**. Provider engages an independent third-party organization to perform penetration testing of Provider systems annually.

d. **Business Continuity**. Provider tests its business continuity and disaster response plan annually.

10. **Data Subject Requests** *(Clause 10(b) SCC)*. During the applicable term of the Agreement, Customer may access, extract, and delete Customer Data from the SaaS Services in accordance with the Documentation to respond to data subjects' requests to exercise one or more of their rights available under Data Protection Laws.

SCHEDULE 4 TO DPA
CROSS BORDER TRANSFER MECHANISM

1. Definitions.

"**EEA**" means the European Economic Area.

"**EU Standard Contractual Clauses**" means the Standard Contractual Clauses approved by the European Commission in decision 2021/914.

"**UK International Data Transfer Agreement**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force 21 March 2022.

2. Applicability. This Schedule will apply when Customer's use of the Services requires the transfer of Personal Data from the EEA, the United Kingdom, or Switzerland to another jurisdiction.

3. Cross Border Data Transfer Mechanisms.

3.1. *Order of Precedence*. In the event the Services are covered by more than one Transfer Mechanism, the transfer of Personal Data will be subject to a single Transfer Mechanism in accordance with the following order of precedence: (a) the EU Standard Contractual Clauses as set forth in Section 3.2 (EU Standard Contractual Clauses) of this Schedule; (b) the UK International Data Transfer Agreement as set forth in Section 3.3 (UK International Data Transfer Agreement) of this Schedule; and, if neither (a) nor (b) is applicable, then (c) other applicable data Transfer Mechanisms permitted under Data Protection Law.

3.2. *EU Standard Contractual Clauses*. The parties agree that the EU Standard Contractual Clauses will apply to Personal Data that is transferred via the Services from the EEA or Switzerland, either directly or via onward transfer, to any country or recipient outside the EEA or Switzerland that is not recognized by the European Commission (or, in the case of transfers from Switzerland, the competent authority for Switzerland) as providing an adequate level of protection for Personal Data. For data transfers from the EEA that are subject to the EU Standard Contractual Clauses, the EU Standard Contractual Clauses will be deemed entered into (and incorporated into this Addendum by this reference) and completed as follows:

(a) Module One (Controller to Controller) of the EU Standard Contractual Clauses will apply where Provider is processing Customer Account Data;

(b) Module Two (Controller to Processor) of the EU Standard Contractual Clauses will apply where Customer is a Controller of Customer Data and Provider is processing Customer Data;

(c) Module Three (Processor to Processor) of the EU Standard Contractual Clauses will apply where Customer is a processor of Customer Data and Provider is processing Customer Data on behalf of Customer;

(d) Module Four (Processor to Controller) of the EU Standard Contractual Clauses will apply where Customer is a Processor of Customer Data and Provider processes Customer Account Data; and

(e) For each Module, where applicable:

i. in Clause 7 of the EU Standard Contractual Clauses, the optional docking clause will not apply;

ii. in Clause 9 of the EU Standard Contractual Clauses, Option 2 will apply and the time period for prior written notice of sub-processor changes will be as set forth in Section 4.b (Current Subprocessors and Notification of Subprocessor Changes) of this Addendum;

iii. in Clause 11 of the EU Standard Contractual Clauses, the optional language will not apply;

iv. in Clause 17 (Option 1), the EU Standard Contractual Clauses will be governed by Irish law;

v. in Clause 18(b) of the EU Standard Contractual Clauses, disputes will be resolved before the courts of Ireland;

vi. in Annex I, Part A of the EU Standard Contractual Clauses:

- Data Exporter: Customer
- Data Exporter Contact details: Set forth in the Order Form
- Data Exporter Role: Controller
- Signature and Date: By entering into the Agreement, Data Exporter is deemed to have signed these EU Standard Contractual Clauses incorporated herein, including their Annexes, as of the effective date of the Agreement.

- Data Importer: Provider, as defined in the preamble to the Agreement.
- Data Importer Contact details: Set forth at the top of the Order Form.
- Data Importer Role: Processor
- Signature and Date: By entering into the Agreement, Data Importer is deemed to have signed these EU Standard Contractual Clauses, incorporated herein, including their Annexes, as of the effective date of the Agreement;

vii. in Annex I, Part B of the EU Standard Contractual Clauses:

- The categories of data subjects are located in Section 1 of Schedule 1;
- The Special Categories of Personal Data transferred are located forth in Section 3 of Schedule 1;
- The frequency of the transfer is a continuous basis for the duration of the Agreement;
- The nature of the processing is located in Section 6 of Schedule 1;
- The purpose of the processing is located in Section 7 of Schedule 1;
- The period for which the Personal Data will be retained is located in Section 8 of Schedule 1;
- For transfers to sub-processors, the subject matter, nature, and duration of the processing are located in Schedule 2; and
- in Annex I, Part C of the EU Standard Contractual Clauses: The Irish Data Protection Commission will be the competent supervisory authority.

viii. Schedule 3 (Technical and Organizational Security Measures) of this Addendum serves as Annex II of the EU Standard Contractual Clauses.

ix. Notwithstanding anything to the contrary, in the event of a conflict between Clause 12 of the EU Standard Contractual Clauses and Section 8 of the DPA, Clause 12 will prevail.

3.3. *UK International Data Transfer Agreement*. The parties agree that the UK International Data Transfer Agreement will apply to Personal Data that is transferred via the Services from the United Kingdom, either directly or via onward transfer, to any country or recipient outside of the United Kingdom that is not recognized by the competent United Kingdom regulatory authority or governmental body for the United Kingdom as providing an adequate level of protection for Personal Data. For data transfers from the United Kingdom that are subject to the UK International Data Transfer Agreement, the UK International Data Transfer Agreement will be deemed entered into (and incorporated into this Addendum by this reference) and completed as follows:

(a) In Table 1 of the UK International Data Transfer Agreement, the parties' details and key contact information is located in Section 3.3 (e)(vi) of this Schedule 4.

(b) In Table 2 of the UK International Data Transfer Agreement, information about the version of the Approved EU SCCs, modules and selected clauses which this UK International Data Transfer Agreement is appended to is located in Section 3.2 (EU Standard Contractual Clauses) of this Schedule 4.

(c) In Table 3 of the UK International Data Transfer Agreement:

i. The list of parties is located in Section 3.2(e)(vi) of this Schedule 4;

ii. The description of the transfer is located in Sections 6 and 7 (Nature and Purpose of the Processing) of Schedule 1 (Details of the Processing);

iii. Annex II is located in Section 9 of Schedule 3 (Technical and Organizational Security Measures); and

iv. The list of sub-processors is located in Schedule 2 of this Addendum.

(d) In Table 4 of the UK International Data Transfer Agreement, both the Importer and the exporter may end the UK International Data Transfer Agreement in accordance with the terms of the UK International Data Transfer Agreement.

3.4. *Conflict*. To the extent there is any conflict or inconsistency between the EU Standard Contractual Clauses or UK International Data Transfer Agreement and any other terms in this Addendum, the Agreement, or the Asymbl Privacy Notice, the provisions of the EU Standard Contractual Clauses or UK International Data Transfer Agreement, as applicable, will prevail.