AnywhereNow Dialogue Cloud Neo Agreement (V3 and above)

This Software as a Service (SaaS) Agreement ("Agreement") is entered into by CUSTOMER on the Effective Date, either directly with WSP or indirectly through a Partner, and governs CUSTOMER's purchase and use of WSP's proprietary SaaS Services and/or associated Support Services, as identified in an Order (all as defined below).

Note that by executing an Order for the purchase of SaaS Services or otherwise using the SaaS Services, CUSTOMER shall be deemed to confirm its acceptance of this Agreement and CUSTOMER's agreement to be a party to this binding contract. if the individual accepting this Agreement is accepting on behalf of a company or other entity, such individual represents that they have authority to bind such entity to this Agreement.

This Agreement shall be interpreted and applied in accordance with Sections 1 and 2.

1 INTERPRETATION AND DEFINITIONS.

1.1 In this Agreement, unless the context otherwise requires:

1. Reference to the parties include their respective successors and permitted assigns;
2. Words in the singular include the plural and in the plural include the singular;
3. Headings are for ease of reference only;
4. Any reference to "Agreement" also refer to any amendment or supplement to it;
5. The term "including" means including without limitation;
6. Capitalised words, phrases and acronyms shall have the meanings given to them in the Agreement or shall have their ordinary (technical or other) meaning; and
7. Parties have expressly required the Agreement to be drawn up in English.

1.2 In the case of a conflict between any provision of this (SaaS) Agreement and any other contract documents, the following descending order of precedence shall apply: (1) the provisions of the body of this Agreement, (2) the privacy provisions of Data Processing Addendum (attached hereto as Exhibit 2), (3) the provisions of the Order and, (4) the other attachments, annexes or schedules. In case of a conflict between the provisions of the Service Level Agreement and the provisions of this Agreement, the latter shall prevail.

1.3 "Affiliate" means any entity which directly or indirectly controls, is controlled by, or is under common control of the parent company of, as appropriate, CUSTOMER Group or AN Group. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

1.4 "AN" means, unless another Affiliate has executed the Order, Workstreampeople B.V. with its registered address in Rotterdam, The Netherlands.

1.5 "AnywhereNow Group" or "AN Group" means Anywhere365 Group B.V. and its Affiliates in each case from time to time.

1.6 "AN Software" means, as applicable, the Object Code form of AnywhereNow suite or such other AN software products to which CUSTOMER is provided access as part of the SaaS Services, as identified in an Order, and shall be deemed to include the Documentation.

1.7 "Agreement" means (as the context requires): (i) this SaaS Agreement (including the Exhibits attached hereto), or (ii) the agreement described under (i) and all Orders, further agreements and other contract documents (taken together).

1.8 "Confidential Information": means all information in any medium or format (including written, oral, visual or electronic, and whether or not marked or described as "confidential"), together with all copies, which relates to a party (the "Disclosing Party") or to its employees, officers, customers or suppliers, and which is directly or indirectly disclosed by the Disclosing Party to the other party (the "Receiving Party") in the course of their dealings relating to this Agreement, whether before or after the date of this Agreement. However, the following information is not "Confidential Information" for the purposes of this Agreement: (i) information which is in the public domain other than as a result of breach of this Agreement or any separate confidentiality undertaking between the parties; (ii) information which the

Receiving Party received, free of any obligation of confidence, from a third party which itself was not under any obligation of confidence in relation to that information; and (iii) information which was developed or created independently by or on behalf of the Receiving Party.

1.9 "CUSTOMER" means the (potential) counter party of AN that entered into an Agreement or (directly or indirectly through a Partner) entered into any negotiations regarding such Agreement.

1.10 "Content" means information rightfully obtained by AN from publicly available sources or its third party content providers and made available to CUSTOMER through the Services, beta Services or pursuant to an Order, as more fully described in the Documentation.

1.11 "Customer Data" means electronic data , information, or material that is submitted, transmitted, stored, or otherwise provided to AN's systems through the SaaS Services by or on behalf of the CUSTOMER, the CUSTOMER Group, or their respective End Users. This includes data originating from or processed by computer systems, devices, or infrastructure owned or operated by the CUSTOMER, the CUSTOMER Group, or third-party service providers acting on their behalf. Customer Data expressly excludes any Content as defined in this Agreement. For clarity, Customer Data shall be treated as the confidential information of the CUSTOMER and is subject to the confidentiality obligations set forth herein.

1.12 "CUSTOMER Group" means CUSTOMER and its Affiliates including CUSTOMER.

1.13 "Data Protection Agreement" or "DPA" means the specific provisions to be agreed between the parties pursuant to Section 11.1, if any, for processing of personal data by AN on behalf of CUSTOMER.

1.14 "Data Protection Laws" means in relation to any personal data (if any) which is processed in the performance of this SaaS Agreement, the applicable (local) law(s) or any other (local) regulations, guidelines or policies, instructions or recommendations of any competent governmental authority, including any amendments, replacements, updates or other later versions thereof;.

1.15 "Documentation" means the user guides, tutorials, online help, release notes, printed instructions, reference manuals, requirements and other explanatory materials developed by AN regarding the use or operation of the SaaS Services.

1.16 "Effective Date" means, unless another date is expressly agreed in the Order, the date the Order becomes effective.

1.17 "End User" means, as applicable and unless stated otherwise herein, any person or entity (including, for the avoidance of doubt, any employee or agent of CUSTOMER) authorized by CUSTOMER to access or use the Products.

1.18 "Fair Use Policy" means the fair use policy governing the Support Services attached in Exhibit 1, as may be amended by AN from time to time.

1.19 "Fees" means in respect of each Agreement, the total sum of fees and charges (recurring and/or one off) payable by the CUSTOMER for Products and/or Services as specified in the relevant Order(s) or (if appropriate) to be calculated by AN based on the most current version of the Pricebook.

1.20 "Host" means the computer equipment on which the AN Software is installed, which is owned and operated by AN or its subcontractors.

1.21 "Object Code" means the form of AN Software wherein computer programs are assembled or compiled in magnetic or electronic binary form on software media, which are readable and usable by machines, but not generally readable by humans without reverse-assembly, reverse-compiling, or reverse-engineering.

1.22 "Orders" means an order referencing this Agreement as may be agreed from time to time with AN (or a Partner) identifying the Products and/or Services, Fees and other details of each transaction that is subject to and governed by this Agreement. An Order may consist of either (a) a schedule, quotation, or statement of work that has been signed by both CUSTOMER and AN (or a Partner), and/or (b) if applicable, a purchase order issued by CUSTOMER pursuant to this Agreement (directly or indirectly through a Partner) to order the Products and/or Services on CUSTOMER's behalf, provided that any preprinted terms on a CUSTOMER purchase order or other terms on a purchase order that are inconsistent with or additional to the terms of this Agreement shall be deemed invalid.

1.23 "Partner" means a third party that is authorised by AN on the basis of a separate and valid agreement, to resell the Products and Services to certain End Users.

1.24 "Pricebook" means the pricelist issued by AN to the general business community and/or public as the centralised source of pricing information and license metric (such as, without limitation, the license type) for all Products and Services and other items, all as may be amended from time to time by AN.

1.25 "Products" means the generally available AN Software, as may be amended by AN from time to time. The SaaS Services are a product (not Services) that is licensed against the execution of an Order. Products" excludes any Third Party Software.

1.26 "SaaS Services" means the subscription cloud-based services identified in the Order and that are hosted by AN or its service provider and made available to CUSTOMER (Group) over a network on a term-use basis, as may be amended by AN from time to time.

1.27 "Services" means any services, other than SaaS Services, provided or to be provided by or on behalf of AN pursuant to this Agreement, as identified in an Order.

1.28 "Support Services" means any standard services offered by AN in support of the Product provided or to be provided by or on behalf of AN, as identified in an Order.

1.29 "Service Levels" means the minimum service levels for the SaaS Services as included the Agreement.

1.30 "Subscription Period" means the period(s) specified in an Order and as described in Section 3.7 during which CUSTOMER will have access to and use of the SaaS Services and/or Support Services, as the same may be renewed or extended in accordance with the applicable Order.

1.31 "Third Party Software" means, if appropriate, the non-AN Software referred to as redistributable code that is licensed to AN by third party licensors for redistribution with the AN Software. The redistributable code is the property of AN's licensors, and protected under international copyright, trade secret or other proprietary rights laws, and international treaties.

1.32 "Term" means any initial term or any renewal term of the Agreement as mutually agreed to by the parties in writing from time to time.

2 APPLICABILITY

2.1 This Agreement shall govern all quotes, and Orders between CUSTOMER and AN for SaaS Services. For all other Products and Services, the EULA as published on AN's web site https://www.anywhere.now/terms-conditions ("Website"), shall govern the relevant (non-SaaS) quotes, and Orders between CUSTOMER and AN. The Agreement is also applicable to the negotiations regarding such quotes or agreements, even if said negotiations do not result in the conclusion of an Agreement and will accordingly apply to all future trading relationships with AN, even if they are not communicated as new. AN may from time to time amend the Agreement as published on the Website. By using the SaaS Services, CUSTOMER agrees to be bound unconditionally by the terms and conditions of this Agreement.

2.2 The applicability of any general terms and conditions of CUSTOMER or Partner to any quote, Order or other agreement, said negotiations or the relationship in general, is hereby excluded. Regardless of their form, deviations from or supplements to the Agreement shall only apply if parties explicitly agree to the same in writing.

3 SAAS SERVICES, RESTRICTIONS AND TERM

3.1 **Provision of SaaS Services.** CUSTOMER acknowledges that Products are licensed not sold. Subject to the terms, restrictions and limitations set forth in the Agreement, AN hereby grants to CUSTOMER a non-exclusive, non-transferable, non-sublicensable, terminable license to access and use (and to permit its End Users to access and use) the SaaS Service during the Subscription Period in accordance with the Documentation, solely for Customer Group's internal business operations. CUSTOMER agrees that its purchase of the Services is neither contingent upon the delivery of any future functionality or features nor dependent upon any oral or written public comments made by AN with respect to future functionality or features.

3.2 **Required software.** CUSTOMER acknowledges that: (i) AN's SaaS Services are designed to operate in conjunction with Microsoft Teams and Azure Communication Services, which are Third party Software that is licensed and operated by Microsoft Corporation or its affiliates, and (ii) the use of Microsoft Teams, Azure Calling, and any associated telephony features including call traffic termination, phone number provisioning, emergency calling, and regulatory compliance is governed solely by Microsoft's applicable license terms and service agreements. The use of the SaaS Service may require the purchase and installation of any Third Party Software licenses as a pre-requisite for using the SaaS Service, as specified in the Documentation and/or as advised by AN or Partner from time to time ("Required

Software") CUSTOMER agrees to install such Required Software, including any required updates if and when available at its own cost and risk.

3.3 **End Users.** Customer is responsible for: (i) all activities conducted by it or through the accounts of its End Users on the SaaS Service and (ii) (as appropriate) maintaining valid licenses for all Third Party Software, functionality, platforms and the likes, including Microsoft Teams and Azure Communication Services, used in conjunction with the SaaS Services. CUSTOMER shall ensure that the End Users shall abide by the terms of this Agreement. Any breach by an End User will be deemed to be a breach by CUSTOMER. AN may terminate or suspend any End User's access to the SaaS Service for any breach without notice.

3.4 **Restrictions.** CUSTOMER and its End Users shall not, and shall not permit any third party to: (i) copy or republish the SaaS Services or AN Software, (ii) make the SaaS Services available to any person other than properly authorised End Users, (iii) use or access the SaaS Services to provide service bureau, time-sharing or other computer hosting services to third parties,(iv) modify or create derivative works based upon the SaaS Services or Documentation, (v) remove, modify or obscure any copyright, trademark or other proprietary notices contained in the software used to provide the SaaS Services or in the Documentation, (vi) reverse engineer, decompile, disassemble, or otherwise attempt to derive the source code of the Software used to provide the SaaS Services, except and only to the extent such activity is expressly permitted by applicable law, or (vii) access the SaaS Services or use the Documentation in order to build a similar product or competitive product. Subject to the limited licenses granted herein, AN shall own all right, title and interest in and to the Software, services, Documentation, and other deliverables provided under this Agreement, including all modifications, improvements, upgrades, derivative works and feedback related thereto and intellectual property rights therein. Customer agrees to assign all right, title and interest it may have in the foregoing to AN.

3.5 **Service Level Agreement.** Parties may agree a Service Level Agreement in a format advised by AN. AN implements a Fair Usage Policy as part of its Support Services to help ensure that all End Customers enjoy high levels of service and in order to protect AN's network and Support Services against misuse and abuse.

3.6 **Customer feedback.** AN may from time to time request CUSTOMER to provide certain information or content by which the End User can be identified when using the SaaS Service including the control panel, and the registration functionality that are compatible with the AN Software. AN will only use and protect such information in accordance with the AN privacy policy available at AN's website https://www.anywhere.now/privacy-policy. AN shall have a royalty-free, worldwide, irrevocable, perpetual license to use and incorporate into the SaaS Services any suggestions, enhancement requests, recommendations or other feedback provided by Customer, including End Users, relating to the operation of the SaaS Services.

3.7 **Term and Subscription Period.** The term of this Agreement shall begin on the Effective Date. The Subscription Period shall accordingly commence on the Effective Date and continues for an initial term of thirty-six (36) months. If an Order is not terminated sooner for cause pursuant to Section 10.1, the Subscription Period shall automatically renew at the end of the initial term and shall thereafter continue for successive annual periods until terminated by either party upon not less than sixty (60) days' written notice prior to the expiration of the then current renewal term.

4 CUSTOMER RESPONSIBILITIES

4.1 **Assistance.** CUSTOMER shall provide commercially reasonable information and assistance to AN to enable AN to deliver the SaaS Services. Customer acknowledges that AN's ability to deliver the SaaS Services in the manner provided in this Agreement may depend upon the accuracy and timeliness of such information and assistance.

4.2 **Compliance with Laws.** CUSTOMER shall comply with all applicable local, state, national and foreign laws in connection with its use of the SaaS Services, including those laws and regulations related to data privacy, international communications, and the transmission of technical or personal data. Customer acknowledges that AN exercises no control over the content of the information transmitted by CUSTOMER through the SaaS Services including the Customer Data and any Third Party Software. CUSTOMER shall and ensure the End Users shall not upload, post, reproduce or distribute any information, software or other material protected by copyright, trade secret, trade mark, privacy rights,

or any other intellectual property right without first obtaining the permission of the owner of such rights.

4.3 **Acceptable Use and ID Information.** Customer shall: (i) notify AN immediately of any unauthorised use of any password or user id or any other known or suspected breach of security, (ii) report to AN immediately and use reasonable efforts to stop any unauthorised use of the SaaS Services that is known or suspected by CUSTOMER or any End User, and (iii) not provide false identity information to gain access to or use the SaaS Services, and (iv) and ensure the End Users shall only use telephone numbers for which they have proper authorization to operate. CUSTOMER is not permitted to use fabricated, placeholder, or otherwise non-operational telephone numbers, including those intended solely for testing purposes**.**

4.4 **Administrator Access.** CUSTOMER shall be solely responsible for the acts and omissions of its End Users with an administrator role. AN shall not be liable for any loss of data or degradation of functionality or other adverse impact caused directly or indirectly by the acts or omissions of administrator End Users. AN shall furthermore not be liable for the accuracy, validity, or legality of any rights, identity verification, or use of telephone numbers, email functionality, or other integrations in connection with any Third Party Software and/or Customer Data.

4.5 **Customer Data.** Except for AN's obligations described in Section 6 and Section 11, CUSTOMER shall have sole responsibility for: (i) the accuracy, quality, and legality of the Customer Data and the means by which Customer acquired the Customer Data and the right to provide the Customer Data for the purposes of this Agreement (including ensuring the receipt of all permissions from individuals and other third parties as may be necessary in order to provide the Customer Data for the purposes contemplated in this Agreement); (ii) the security and confidentiality of CUSTOMER's and its End Users' account information; (iii) maintaining a back-up of all Customer Data; (iv) preventing unauthorized access to, or use of, the SaaS Services including to process Customer Data, and notify AN promptly of any such unauthorized access or use; (v) collecting, inputting and updating all Customer Data stored on the Host, (vi) ensuring that the Customer Data does not include anything that actually or potentially infringes or misappropriates the copyright, trade secret, trademark or other intellectual property right of any third party or contain anything that is obscene, defamatory, harassing, offensive or malicious, and (vii) collecting and handling all Customer Data in compliance with all applicable Data Protection Laws, rules, and regulations.

4.6 **License from Customer.** Subject to the terms and conditions of this Agreement, CUSTOMER shall grant to AN a limited, non-exclusive and non-transferable license, to copy, store, configure, perform, display and transmit Customer Data solely as necessary to provide the SaaS Services to CUSTOMER.

4.7 **Ownership and Restrictions.** CUSTOMER retains ownership and intellectual property rights in and to its Customer Data, AN or its licensors retain all ownership and intellectual property rights to the services, Software programs, and anything developed and delivered under the Agreement.

5 FEES, PAYMENT AND TAXES.

5.1 **Fees and Adjustments.** Unless otherwise provided in an Order, AN shall invoice CUSTOMER for all Fees due on or promptly following the Effective Date. During the Subscription Period, CUSTOMER agrees to pay the annual Fee for the SaaS Services and the Support Service as well as the Fee for any other Products or Services, all as specified in the Order (or if no order was agreed, the then current Pricebook will apply). Upon renewal, the Fees shall be calculated based on the then-current Pricebook or as otherwise advised to the CUSTOMER in writing at least sixty (60) days prior to the renewal date. For any renewal term, Fees may be adjusted to reflect changes in the applicable Pricebook including (if appropriate) inflationary adjustments generally applied by AN during the initial term. Any discounts or incentives applied during the initial term shall not automatically carry forward into any renewal term unless expressly agreed in writing in a renewal Order. Except as expressly provided otherwise herein, Fees are non-refundable, non-cancellable and not subject to set-off. All Fees shall be paid by Customer in the currency stated in each Order. During the Term, AN may from time to time adjust the Fees including recurring (SaaS) Fees annually for inflation.

5.2 **Purchases Through a Partner.** For any Products or Services purchased by CUSTOMER through a Partner, the pricing and payment terms are established through the order or agreement entered into by and

between CUSTOMER and the Partner ("Partner Order") and all payments will be made directly to Partner.

5.3 **Payment and Payment term.** CUSTOMER shall pay an invoice from AN within 30 days from the date of issuance. AN shall issue its invoice when: (a) it receives the Order from CUSTOMER, (b) the agreed (periodic) invoice date(s) has (have) elapsed. A late payment charge of the lesser of 1.5% per month or the highest interest rate allowed by applicable law will be charged upon all past due amounts hereunder.

5.4 **Taxes and Duties.** Prices to CUSTOMER do not include taxes, duties, tariffs, handling fees, or other such assessments of any nature. Whenever imposed, such assessments are payable by CUSTOMER. Income or other taxes that are required to be paid or withheld by CUSTOMER or AN under the laws of jurisdictions other than The Netherlands, in connection with the Fees paid by CUSTOMER hereunder, are the sole obligation of CUSTOMER and shall be exclusive of the Fees paid by CUSTOMER.

6 CONFIDENTIAL INFORMATION, TITLE AND COPYRIGHTS.

6.1 **Confidential Information.** Each Disclosing Party shall maintain strict confidentiality with regard to any Confidential Information disclosed to the Receiving Party. It shall deploy such procedures with regard to Confidential Information that shall be no less restrictive than the strictest procedures used by it to protect its own confidential and proprietary information, but not less than reasonable care. Each party acknowledges that a breach of this obligation will constitute a material breach of the Agreement and will lead to liability on its part. Each party shall ensure that its personnel or (the personnel of) any subcontractors are advised of the confidential and proprietary nature of the Confidential Information and are bound in writing to confidentiality obligations no less strict than as set out in this Agreement. During the term of this Agreement, any Confidential Information disclosed will be protected for a period of three (3) years from date of disclosure (perpetually in the case of intellectual property), each party shall treat as confidential all Confidential Information of the other party, shall not use such Confidential Information except to exercise its rights and perform its obligations under this Agreement, and shall not disclose such Confidential Information to any third party. Without limiting the foregoing, each party shall use at least the same degree of care, but not less than a reasonable degree of care, it uses to prevent the disclosure of its own confidential information to prevent the disclosure of Confidential Information of the other party. Neither party shall reverse engineer, disassemble or decompile any prototypes, software or other tangible objects which embody the other party's Confidential Information and which are provided to the party hereunder.

6.2 **Notifications.** Each party shall promptly notify the other party of any actual or suspected misuse or unauthorised disclosure of the other party's Confidential Information.

6.3 **Title.** CUSTOMER acknowledges that the AN Software (including , any enhancements, modifications, additions) contains confidential information of, are trade secrets of, and are proprietary to AN and its licensors. CUSTOMER shall not assert any right, title or interest in the AN Software or other materials provided to CUSTOMER under this Agreement, except for the limited license rights expressly granted to CUSTOMER in Section 3.

6.4 **Copyright.** CUSTOMER shall not obscure or remove any copyright or other proprietary notice or legend contained on or included in the AN Software and shall reproduce all such information on all copies made hereunder. CUSTOMER shall not, directly or indirectly, disclose or distribute any technical information of AN provided with or in the AN Software without the prior written consent of AN, which consent may be withheld at AN's sole discretion.

7 LIMITED WARRANTIES.

7.1 **Product Warranty.** Provided that CUSTOMER is not in breach of any of its obligations under this Agreement, AN warrants from the Effective Date that (i) AN has validly entered in this Agreement and has the legal power to do so, (ii) AN will provide the SaaS Services in a professional manner consistent with general industry standards and that the SaaS Services will perform substantially in accordance with the Documentation and (iii) the overall functionality of the SaaS Services will not materially decrease during the Subscription Period.

7.2 **Disclaimer of Warranties.** AN and its licensors make no warranty, representation or promise except as specifically set forth in this Agreement. to the fullest extent permitted by law, AN does not guarantee that the SaaS Services will: (i) be performed error-free or uninterrupted, or (ii) that AN will correct all SaaS Services errors, or (iii) will satisfy CUSTOMER's requirements. CUSTOMER acknowledges that AN does not control the transfer of data over communications facilities, including the Internet, and that the SaaS Service may be subject to limitations, delays, and other problems inherent in the use of such communications facilities. This Section 7 sets forth the sole and exclusive warranty given by AN (express or implied) with respect to the subject matter of this Agreement. Neither AN nor any of its licensors or other suppliers warrant or guarantee that the operation of the SaaS Services will be uninterrupted, virus-free or error-free, nor shall AN or any of its service providers be liable for unauthorised alteration, theft or destruction of CUSTOMER's or any User's data, files, or programs

7.3 **Excusive Remedy.** As CUSTOMER's sole and exclusive remedy and AN's entire liability for any breach of the warranty set forth in Section 7.1, CUSTOMER's exclusive remedy shall be as provided in Section 10.

7.4 **Exclusions from Warranty.** The limited warranty is void if non-conformance of the AN Software results from or is related to the:

1. factors outside of our reasonable control (for example, natural disaster, war, acts of terrorism, riots, government action, or a network or device failure outside our control);
2. use of hardware, or software not provided or not approved (as recommended in the Documentation) by or on behalf of AN, including, but not limited to, issues from inadequate bandwidth, high latency or related to third-party software or services resulting
3. use of AN Software after advice was given to modify your use of the AN Software and provided CUSTOMER did not modify its use as advised;
4. unauthorized action or lack of action when required, or from CUSTOMER's employees, agents, contractors, or vendors, or anyone gaining access to AN's network by means of CUSTOMER's passwords or equipment, or otherwise resulting from a failure attributable to CUSTOMER to follow appropriate security practices;
5. CUSTOMER's failure to adhere to any required configurations, install Required Software, use supported platforms, follow any policies for acceptable use, or CUSTOMER's use of the Saas Services in a manner inconsistent with AN's published guidance;
6. CUSTOMER's faulty input, instructions, or arguments (for example, requests to access files that do not exist);
7. CUSTOMER's attempts to perform operations that are not permitted or supported by the Documentation; or
8. Products or Services for which CUSTOMER at the time of the claim has not or not fully paid.

7.5 **Try & Buy.** If the AN Software is purchased as a trial or evaluation version, a limited license will be granted to use certain key functionality of the Software on an "AS IS" basis for your own internal evaluation purposes and during a limited period of maximum thirty (30) calendar days and otherwise subject to the express limitations of the trial. Unless CUSTOMER and AN agree otherwise in writing prior to the expiration or termination of the trial period, CUSTOMER agrees to cease all use of the AN Products and Services.

8 LIMITATION OF LIABILITY.

8.1 WITHOUT PREJUDICE TO SECTION 8.2 BELOW, TO THE MAXIMUM EXTENT PERMITTED BY LAW, AN'S AGGREGATE LIABILITY ARISING FROM OR RELATING TO THE LICENSE, PRODUCTS OR SERVICES PROVIDED UNDER THIS AGREEMENT, IRRESPECTIVE OF THE NATURE OF THE CLAIM, IS LIMITED TO THE FEES ACTUALLY PAID OVER THE CONTRACT YEAR (EXCLUSIVE VAT) IN WHICH THE DAMAGE CAUSING EVENT OR, IN CASE OF A SERIES OF RELATED EVENTS, THE FIRST DAMAGE CAUSING EVENT OCCURRED OR COMMENCED.

8.2 IN NO EVENT SHALL AN OR ITS LICENSORS BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, PUNITIVE OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR ANY OTHER PECUNIARY LOSS). IT IS SPECIALLY UNDERSTOOD AND AGREED THAT AN EXCLUDES LIABILITY FOR (I) ANY FAILURE BY AN TO MEET AGREED SERVICE LEVELS FOR THE SAAS SERVICE AS A RESULT OF NETWORK

INTRUSIONS AND/OR INCIDENTS ATTRIBUTABLE TO CRITICAL IT SERVICE PROVIDERS INCLUDING MICROSOFT CORP (AZURE) , AND (II) CLAIMS IN CONNECTION WITH CUSTOMER DATA INCLUDING BY THIRD PARTIES ENGAGED BY OR ON BEHALF OF CUSTOMER GROUP TO PERFORM OWNERESHIP VALIDATION OF TELEPHONE NUMBERS. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMIT ACTION OF INCIDENT AL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY. ANY LIMITATION OR EXCLUSION OF LIABILITY AS SET OUT IN SECTION 8.1 OF THE AGREEMENT SHALL NOT APPLY IN SO FAR AS THE DAMAGE IS CAUSED BY: (I) GROSS NEGLIGENCE OR WILFUL MISCONDUCT, OR (II) PERSONAL OR FATAL INJURY, OR (III) IP INFRINGEMENT CLAIMS AS DECRIBED IN SECTION 9.1.

9 INDEMNITIES AND CUSTOMER OBLIGATIONS

9.1 Infringement Indemnity: Subject to Section 9.2 and the restrictions and limitations set forth herein, AN shall indemnify and hold harmless CUSTOMER from and against any costs or demands awarded against CUSTOMER by a court of competent jurisdiction pursuant to a final judgment as a result of a claim or action by a third party against CUSTOMER that the SaaS Service or Documentation infringes a registered copyright, trademark, valid patent or other intellectual property right of a third party in North America, European Economic Area, the United Kingdom or Japan. The indemnity is conditioned on CUSTOMER:

A. promptly notifying AN of such claim;
B. permitting AN to control the response thereto and the defence thereof, including any agreement relating to the settlement thereof, and
C. assisting and cooperating with AN in the defence or settlement thereof. CUSTOMER may participate, at its own expense, in such defence directly or through counsel of its choice on a monitoring, noncontrolling basis. AN shall obtain CUSTOMER’s prior written consent to any compromise or settlement of any claim which would require an admission of liability on the part of CUSTOMER or which would subject CUSTOMER to any injunction or other equitable relief.

9.2 CUSTOMER Indemnity. To the extent permitted by applicable law, if a third party makes a claim against AN to the extent it alleges that: (i) any Customer Data, Third Party Software hosted in an Online Service by AN on CUSTOMER's behalf misappropriates a trade secret or directly infringes a patent, copyright, trademark, or other proprietary right of a third party; or (ii) CUSTOMER’s use of any Product, alone or in combination with anything else (including any non-AN Product), violates the law or harms a third party; or (iii) the use of telephone numbers by Customer, its End Users, or contractors without proper legal authorization, including but not limited to the use of fabricated, placeholder, or otherwise non-operational numbers, CUSTOMER shall defend AN and its directors, officers and employees against the claim at CUSTOMER’s expense and CUSTOMER shall pay all Loss finally awarded against such parties or agreed to in a written settlement agreement signed by CUSTOMER, to the extent arising from the claim.

9.3 Exclusions. AN shall have no obligation under Section 9.1, and otherwise will have no liability for, any claim of infringement caused or alleged to be caused by:

A. Customer Content, Third Party Software hosted in an Online Service by AN on CUSTOMER's behalf;
B. modifications of the SaaS Services not authorised by AN, or;
C. use of the SaaS Services other than in accordance with the Documentation and this Agreement.

9.4 AN may, at its sole option and expense, procure for CUSTOMER the right to continue use of the SaaS Services, modify the SaaS Services in a manner that does not materially impair the functionality, or terminate the subscription/ Term and repay to CUSTOMER any amount paid by CUSTOMER with respect to the subscription following the termination date.

9.5 Exclusive Remedy: Without prejudice to section 9.3, the foregoing Sections 9.1 and 9.2 set forth the exclusive remedy and entire liability and obligation of AN with respect to third party claims against CUSTOMER alleging intellectual property infringement or misappropriation.

9.6 Injunctions. In the event that a claim of infringement of a valid North American, European Economic Area, the United Kingdom or Japanese software patent or copyright is made against AN or CUSTOMER or if AN reasonably believes that such a claim will be made, AN, at its option and in lieu of indemnification, may:

A. procure for CUSTOMER the right to use the AN Software without patent or copyright infringement;
B. modify the AN Software to make it non-infringing;
C. replace the AN Software with substantially equivalent software that is non-infringing; or
D. direct CUSTOMER to cease use of the AN Software, and refund to CUSTOMER a percentage of the aggregate fees received for such AN Software that are the subject of such a claim, based on a five (5) year straight line depreciation.

9.7 CUSTOMER Obligations. CUSTOMER is solely responsible for:

A. its use of the SaaS Services, including ensuring a level of security appropriate to the risk in respect of the Customer Data, securing its account authentication credentials, protecting the security of Customer personal data when in transit to and from the SaaS Services, taking appropriate steps to securely encrypt and/or backup any Customer personal data uploaded to the SaaS Services, and properly configuring the SaaS Services and using available features and functionalities to maintain appropriate security in light of the nature of the Customer personal data processed by CUSTOMER's use of the SaaS Services; and

B. the Customer Data that CUSTOMER (Group) elects to store or transfer outside of AN's and (if appropriate) its sub-processors' systems (for example, offline or on-premise storage). AN has no obligation to protect such data; and

C. reviewing the security measures and evaluating for itself whether the SaaS Services and the security measures and AN's commitments in respect of data processing will meet CUSTOMER's needs, including with respect to any obligations of CUSTOMER under data protection laws, as applicable.

D. not allowed to give any third parties/agents access to Products and/or SaaS Services provided to the CUSTOMER which are hosted by or on behalf of AN. CUSTOMER shall, during the Term, allocate sufficient third party software licenses as required to run (as appropriate) the AN Software or the Software as a Service in accordance with the Documentation.

E. engaging any telephony providers to operate its telephony services and acknowledges that AN is not a licensed telecommunications provider under applicable laws. CUSTOMER is and remains responsible for validating, verifying, or ensuring the legal authorization or ownership of any telephone numbers used by CUSTOMER or its End Users including, by way of example, obligations under the EU Electronic Communications Code and the North American Numbering Plan (NANP).

10 TERMINATION.

10.1 Termination for Breach. Each party will have the right to terminate this Agreement (in whole or in part) at any time by giving written notice to the other party if (i) the other party breaches any material term of this Agreement and fails to cure such breach within thirty (30) days after written notice thereof; (ii) the other party repeatedly breaches any terms of this Agreement in such manner as to reasonably justify the opinion that its conduct is inconsistent with it having the intention or ability to give effect to the terms of this agreement, (iii) if any of the following events occur: (a) the presentation of a petition for winding up (b) is the subject of an order or an effective resolution is passed for winding up; (c) the application for an order or application for the appointment of a receiver (including an administrative receiver), administrator, trustee or similar officer in respect thereof; (d) if a receiver, administrative receiver, administrator or similar office is appointed over all or any part of the assets or undertaking; (e) making a composition with its creditors generally or an assignment for the benefit of its creditors or other similar arrangement; (f) goes into liquidation; or (g) ceasing, or threatening to cease, to carry on business.

10.2 Suspension for Non-Payment. AN reserves the right to suspend delivery of the SaaS Services if CUSTOMER fails to timely pay any undisputed amounts due to AN under the Agreement, but only after AN

notifies CUSTOMER of such failure and such failure continues for thirty (30) days or more after the payment due date. Suspension of the SaaS Services shall not release CUSTOMER of its payment obligations under this Agreement. CUSTOMER agrees that AN shall not be liable to CUSTOMER or to any third party for any liabilities, claims or expenses arising from or relating to suspension of the SaaS Services resulting from CUSTOMER's non-payment.

10.3 Suspension for Ongoing Harm. AN reserves the right to suspend delivery of the SaaS Services if AN reasonably concludes that CUSTOMER or an End User's use of the SaaS Services is causing immediate and ongoing harm to AN or others. In the extraordinary case that AN must suspend delivery of the SaaS Services, AN shall immediately notify CUSTOMER of the suspension and the parties shall diligently attempt to resolve the issue. AN shall not be liable to Customer or to any third party for any liabilities, claims or expenses arising from or relating to any suspension of the SaaS Services in accordance with this Section 10.3. Nothing in this Section 10.3. will limit AN's rights under Section 10.5 below.

10.4 Exclusive Reasons for Termination. To the extent permitted by law, the parties waive any right to terminate, rescind, or otherwise end the Agreement, on grounds other than those set out herein.

10.5 Effect of Termination.

A. Upon expiration or termination of this Agreement AN shall immediately cease providing the SaaS Services and all usage rights granted under this Agreement shall terminate.

B. If AN terminates this Agreement due to a material, uncured breach by CUSTOMER, then CUSTOMER shall immediately pay to AN or Partner (if purchased through a Partner) all amounts then due or to become due during any Order issued under. If CUSTOMER terminates this Agreement due to an uncured material breach by AN, then AN shall immediately refund to CUSTOMER all pre-paid amounts for any unperformed SaaS Services scheduled to be delivered for the remainder of the (Initial) Subscription Period.

C. Upon termination of this Agreement and upon subsequent written request by the disclosing party, the receiving party of tangible Confidential Information shall promptly return such information or destroy such information and provide written certification of such destruction, provided that the receiving party may permit its legal counsel to retain one archival copy of such information in the event of a subsequent dispute between the parties.

10.6 Termination of Orders. Unless agreed otherwise, all Orders issued under this Agreement shall terminate immediately on termination of this Agreement in accordance with this section 10.

11 PERSONAL DATA AND PRIVACY

11.1 Scope. The parties will comply with Data Protection Laws relating to WSP's processing of CUSTOMER GROUP personal data as part of the SaaS Services provided pursuant to this Agreement. The further details are set forth in the Data Processor Addendum, attached as Exhibit 2, which will form part of this Agreement. If no separate Data Processor Agreement is executed, this Agreement will be considered a data processing agreement as defined under Data Protection Laws.

12 GENERAL.

12.1 Non-Exclusive Service. CUSTOMER acknowledges that SaaS Services are provided on a non-exclusive basis. Nothing shall be deemed to prevent or restrict WSP's ability to provide the SaaS Services or other technology, including any features or functionality first developed for CUSTOMER, to other parties.

12.2 License administration and Audit. CUSTOMER shall keep complete and accurate books and records of its use of the SaaS Services to demonstrate its compliance with this Agreement. Further, WSP may audit CUSTOMER's use of the SaaS Services in order to verify compliance with this Agreement.

12.3 Notices. Any notice required or permitted to be given by CUSTOMER hereunder shall be in writing and delivered by courier or overnight delivery services, by email (with a read-receipt) or by certified mail, and in each instance will be deemed given upon receipt. Any such notice shall be delivered or sent to WSP, Van Nelleweg 1, 3044 BC Rotterdam, The Netherlands.

12.4 Governing Law and Disputes.

A. United States. If you acquired the WSP Software or Services in the United States, all matters arising from or connected with this Agreement, are governed by New York state law, excluding the United Nations Convention on the International Sale of Goods ("CISG"), conflict of law rules and choice of law principles that provide otherwise.

B. Outside the United States. If you acquired the WSP Software or Services in any other country outside the United States, all matters arising from or connected with this Agreement, are governed by the laws of the Netherlands, excluding CISG, conflict of law rules and choice of law principles that provide otherwise.

C. Disputes. Any dispute between CUSTOMER and WSP with regard to this Agreement shall exclusively be submitted to the courts of New York if you acquired the WSP Software or Services in the United States. In all other cases, such dispute shall be exclusively settled by arbitration in The Hague, The Netherlands, in the English language in accordance with then existing Rules of Conciliation and Arbitration of the International Chamber of Commerce ("ICC") by 1 (one) arbitrator to be selected in accordance with the said rules. The parties request the ICC Court of Arbitration to attempt to appoint an arbitrator who is knowledgeable in the area of information technology; if no such arbitrator can be appointed, the normal appointment process shall apply. The award rendered therein shall be final and binding upon the parties to such arbitration proceedings.

D. Urgent relief. CUSTOMER acknowledges and agrees that any copying or use of the WSP Software other than as expressly permitted by this Agreement would result in irreparable injury to WSP for which money damages would be inadequate and in such event submission to arbitration shall not preclude WSP's ability, in addition to other remedies available at law and in equity, to immediate injunctive relief to prevent any such unauthorized use.

12.5 **Legal Effect.** This Agreement describes certain legal rights. You may have other rights under the laws of your state or country. You may also have rights with respect to the party from whom you acquired the WSP Software. This Agreement does not change your rights under the laws of your state or country if the laws of your state or country do not permit it to do so.

12.6 **Assignment.** Neither party may assign any rights, duties, obligations or privileges under this Agreement without the prior written consent of the other party. Furthermore, CUSTOMER may not assign (or pledge) a claim against WSP in a way that is valid under applicable property law without the prior written consent of WSP. A change of control or ownership shall not be deemed to be an assignment under this Section so long as the new owner has expressly assumed in writing all of the duties and obligations of the assignor and further provided, that CUSTOMER shall remain liable and responsible to WSP (and its licensors) for the performance and observance of all such duties and obligations.

12.7 **Severability.** Should any part or provision of this Agreement be held unenforceable or in conflict with the law of any jurisdiction, the validity of the remaining parts or provisions shall not be affected by such holding.

12.8 **Limitation on Effect of Waiver.** Failure on the part of WSP to exercise, or WSP's delay in exercising, any of WSP's rights hereunder shall not be construed as a waiver or waiver of other breaches of this Agreement. Any single or partial exercise by a party of any right shall not preclude any other or future exercise thereof or the exercise of any other right in the Agreement.

12.9 **Entire Agreement and Amendments.** The Agreement contains the entire understanding of the parties with respect to the transactions contemplated and supersedes any prior agreements or understandings among the parties with respect to the subject matter hereof. Except as expressly agreed otherwise in this Agreement, the provisions of the Agreement may be amended only in writing signed by authorised representatives of both parties.

12.10 **Use of Names and Marks**. All names, trademarks, trade names or logo's (collectively "Branding") of each party are and will remain the exclusive property of such party. Neither party will acquire any right to the Branding of the other party. WSP will have the limited right to use CUSTOMER's Branding in connection with the activities described the Purchase Order or to the standard customer section of their corporate websites. Each party will also have the right to include the other party's company name in a standard press release where the company's name is used in a standard list that includes all alliance or vendor members (no exclusive reference to a specific company).

12.11 **Export Law Assurances.** CUSTOMER acknowledges that it is familiar and shall comply with all domestic and international export laws and regulations that apply to the WSP Software. These laws include restrictions on destinations and use. CUSTOMER hereby expressly agrees to defend, hold harmless and indemnify WSP, its directors, officers, and employees, from any claim, suit or dispute alleging that CUSTOMER has exported the WSP Software in violation of such laws.

12.12 **Construction.** The headings in this Agreement are for convenience of the parties only. They do not constitute a portion of this Agreement and shall not be used in interpreting the construction of this Agreement.

12.13 **Third Party Beneficiary.** CUSTOMER hereby agrees that the licensors of Third Party Software shall be considered third party beneficiaries of this Agreement and shall be entitled to bring a direct action against CUSTOMER in the event of breach of any applicable provisions of this Agreement, pursuant to the terms and conditions of this Agreement.

12.14 **Force Majeure.** Neither party shall be in default if failure to perform any obligation hereunder is caused solely by unforeseen supervening conditions beyond that party's reasonable control, which could not have been prevented by the non-performing party's reasonable precautions, commercially accepted processes or substitute services, including acts of God, civil disturbances, strikes and labour disputes.

12.15 **Survival.** The rights and obligations of the parties which by their nature extend beyond the expiration or termination of the Agreement shall survive termination or expiry of this Agreement for any reason.

12.16 **Negation of Agency and Similar Relationships.** Nothing contained in this Agreement shall be deemed to create an agency, joint venture or partnership relationship.

VERSION SAAS AGREEMENT: [2025.08]

Exhibit 1 Fair Use Policy for Support Services

Scope. This document outlines the fair use policy of the support services offered by Workstreampeople B.V. or any of its affiliates (“WSP”, “we” or “our”) for WSP’s Dialogue Cloud services ("Support Services") and accompanies the (SaaS) Agreement we entered into with you ("Customer", “you” or “your”). Capitalised terms used in this Fair Use Policy that are not defined herein have the meanings given to them in the Agreement. This Fair Use Policy solely governs the Support Services.

General: This Fair Use Policy seeks to ensure an optimal and fair, user experience for all our customers. WSP is committed to an up-front, published, simple, transparent, and no-nonsense subscription pricing model. Pricing for WSP’s products and/or services are in our Pricebook. WSP uses all commercially reasonable efforts to ensure its Pricebook is complete and accurate.. We use all commercially reasonable methods to prevent any extra fees/hidden costs when the Support Sservices are used reasonably and normally. However, to maintain that position (the lack of hidden charges) we need to ensure that the provision of the Support Services is transparent and optimal, as well as fair to all our customers.
WSP will monitor this process monthly and will discuss the outcome via a Service Management meeting with the Partner or End Customer. This Fair Use Policy is limited to our Support Services and covers elements including the number of Tickets/issues logged or number of times of WSP staff allocated to Incident response.

As WSP determines the scope of Fair Use we will consider the actual use of the Support Services, your entitlement (Standard or Premium Support), technical advances and the current price rate of all necessary WSP tools/resources.

WSP reserves the right to adjust the Support Fees if the Support Services used by the customer exceed the Fair Use Policy thresholds of 50% or more, for 2+ consecutive months. If WSP detect something out of the ordinary or excessive use in your Support Service usage, WSP will contact you to discuss the situation and potential alternatives. In extreme cases, we may be required to limit the Support Services usage (e.g., limit your access to support). Alternatively, we may discuss with you options to resolve the discrepancy.

Urgent and Extreme Cases. In an urgent or extreme case, for example where Support Services are likely to be significantly impacted, or where we believe your system or ours is under attack (a DDOS - denial of service attack for instance) or where we believe your system or ours has been compromised (for example a hacker or potential a security breach) we may cease the delivery of the Support Services, or temporarily suspend your access to them. Before we do this, we will always contact you to discuss possible solutions. Furthermore we may, irrespective from an attack or breach, if your use of the Support Services continues to adversely affect (in all material respects) other users, or can reasonably be expected to do so, or is generating costs to us that are not normal when compared to other customers on the same support contract and pursuant to this Fair Use Policy, we may require you to execute a follow-up Order to compensate WSP for the increased efforts before continuing the delivery of the Support Services to you. Before we do this, we will always contact you to discuss in good faith possible solutions.

Exhibit 2 Data Processing Addendum

This Data Processing Addendum including its Schedules ("DPA") forms part of the Agreement between WSP and Customer and shall be effective on the effective date of the Agreement ("Effective Date"). All capitalized terms not defined in this DPA shall have the meanings given to them in the Agreement.

1. INTERPRETATION AND DEFINITIONS

Capitalised terms used in this DPA that are not defined in this Section 1 (Interpretation and Definitions) shall have the meaning given to them elsewhere in this DPA and/or the Agreement. The following capitalized terms have the following meaning for the purposes of this DPA:

1.1. "Affiliate" has the meaning set forth in the Agreement, or if no such meaning is given, means any entity which directly or indirectly controls, is controlled by, or is under common control of the parent company of, as appropriate, CUSTOMER Group or WSP Group. "Control," for purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity. In each case where Customer or an Affiliate of Customer purchases Products or Services from WSP hereunder, the term "WSP" wherever used in this DPA shall refer solely to the entity for all purposes relating to the particular WSP Offerings being provided and Order being executed, and the rights, obligations and liabilities relating thereto. For the avoidance of doubt, (A) only the WSP Group entity having executed the Order will have any obligation or liability in connection with or with respect to this DPA, and neither WSP Group' ultimate parent entity nor any Affiliate thereof (other than the entity having executed the Order) will be deemed a party in connection with any Order provided or executed by, or WSP Offerings provided by such entity to Customer; (B) Customer acknowledges that WSP, WSP Group's ultimate parent entity and each Affiliate thereof are each a separate and distinct entity that manages its own affairs; (C) neither WSP, WSP Group' ultimate parent entity nor any Affiliate thereof (other than the entity having executed the Order) shall have any liability or obligation under this DPA; and (D) Customer hereby irrevocably waives any claim it may have against WSP, WSP Group's ultimate parent entity or any other Affiliate thereof (other than the entity having executed the Order) with respect to any WSP Offerings. The WSP Group entity having executed the Order shall be a third party beneficiary of this DPA and shall be entitled to enforce the rights of WSP hereunder. The liabilities and obligations under this DPA of each WSP Group entity that has executed an Order, shall be several and not joint.

1.2. "Agreement" means an agreement in effect between Customer and WSP that governs Customer's use of, and WSP's provision to Customer of, specific Products and Services (as identified in the Order).

1.3. "Customer" means the party identified in the applicable Agreement in effect between WSP and such party.

1.4. "Customer Personal Information" means any Personal Information that is submitted, disclosed, provided or otherwise made available to WSP (either directly or indirectly) by or on behalf of Customer under or in connection with the WSP Offerings.

1.5. "Data Protection Laws" means all data protection and privacy laws applicable to the respective party in its role in the Processing of Personal Information under the Agreement. WSP will never be required to Process Customer Personal Information if prohibited by Data Protection Laws.

1.6. "Marketplace" means an online marketplace operated or controlled by a third party, which is authorised to market and/or distribute WSP Offerings.

1.7. "Order" means WSP's quote, statement of work, or an ordering document (including online order form) accepted by Customer through either: (i) Customer's signature on the WSP or Partner quote; or (ii) the issuance of a purchase order or other ordering document submitted to WSP (directly or indirectly through a Partner or Marketplace) to order the WSP Offerings on Customer's behalf, which references the WSP Offering, pricing and other applicable terms set forth in an applicable WSP quote or ordering document. Orders do not include any preprinted terms on a Customer purchase order or other terms on a purchase order that are inconsistent with or additional to the terms of the Agreement.

1.8. "Other Services" means, collectively or individually, all technical and non-technical consulting and advisory services identified in an Order as Professional Services or Training Services purchased by Customer and performed or delivered by WSP under the Agreement. For purposes of clarity, "Other Services" does not include the SaaS Services, or Support Services.

1.9. "Personal Information" means: any information (i) relating to an identified or identifiable natural person; or (ii) defined as "personally identifiable information", "personal information", "personal data" or similar terms, as such terms are defined under Data Protection Laws.

1.10. "Partner" means a third party that has an agreement with WSP that authorises the third party to resell specific WSP Offerings and Other Services to Customer.

1.11. "Process", "Processes", "Processing", and "Processed" means any operation or set of operations performed upon Customer Personal Information, whether or not by automatic means.

1.12. "Professional Services" means consulting services provided by WSP to Customer that support Customer's deployment, extension and use of WSP Offerings and include, but are not limited to, implementation services, implementation support, best practices consultations, and integration efforts as further described in, and subject to, the Agreement (including the applicable Order).

1.13. "SaaS Services" has the meaning assigned to it in the Agreement.

1.14. "WSP Offerings" means any Dialogue Cloud Products (V3 and above named Dialogue Cloud Neo) and Services made available or otherwise provided by WSP to Customer.

1.15. "Security Incident" means any unauthorised or unlawful breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to Customer Personal Information on systems managed by or otherwise controlled by WSP.

1.16. "Services" means services provided by WSP to Customer, excluding SaaS Services, which may include: (i) Support (Services); (ii) Professional Services; and iii) Other Services provided by WSP to Customer pursuant to the Agreement.

1.17. "Schedule" means each and all schedules, addenda attached to the body of this DPA.

1.18. "Sub-processor" or "Subprocessor" means any entity engaged by WSP or its Affiliates to assist in fulfilling its obligations with respect to providing Services to Customer. Sub-processors may include third parties or WSP's Affiliates. Sub-processors may also include subcontractors that are specified in an applicable statement of work which form part of the Agreement.

1.19. "Support (Services)" means WSP's support and maintenance services for WSP Offerings as described in the Documentation.

1.20. "Training Services" means WSP's courses and other product-related training available through WSP's Identity University, on-site at WSP's, Customer's or a third party's location, or online via a WSP-provided website, as agreed by the parties.

1.21. "WSP" means the WSP Group entity that adopts the Agreement with the Customer.

1.22. "WSP Group" means Anywhere365 Group B.V. and its Affiliates including Anywhere365 LLC, Anywhere365 Ltd, Anywhere365 Spain SA, Anywhere365 Pty Ltd, in each case from time to time

2. JURISDICTION-SPECIFIC ADDENDA

2.1. The Addenda provide terms specific to the Processing of Customer Personal Information arising out of specific legal requirements from particular jurisdictions. In the event that Customer Personal Information is Processed from one or more of these jurisdictions, and the applicable requirements are not already covered in this DPA, then the specific terms in the respective Addendum attached hereto shall apply solely with respect to Customer Personal Information subject to the applicable legal requirements of such jurisdiction(s). In the event of a conflict between the Agreement or this DPA and an Addendum, the Addendum applicable to Customer Personal Information from the relevant jurisdiction shall prevail with respect to Customer Personal Information from that relevant jurisdiction, and solely with regard to the portion of the conflicting provision(s).

2.2. Attached to this DPA is the European Addendum as Schedule B and the United States Privacy Law Addendum as Schedule C. In the event Customer believes Customer Personal Information is processed within the scope of one or more additional jurisdictions, which require additional Addenda to be attached to this DPA, Customer has the sole responsibility for notifying WSP and working with WSP to effectuate such Addenda. Such additional Addenda shall apply subject to the requirements of this Section 2.

3. UPDATES TO DPA.

3.1. When Customer renews or purchases WSP Offerings or Professional Services, the then-current DPA terms will apply during the term of the Order for such WSP Offerings or Professional Services.

3.2. In the event of changes to applicable Data Protection Laws, including, but not limited to, the amendment, revision, or introduction of new laws, regulations, or other legally binding requirements to which either party is subject, WSP may revise the terms of this DPA and issue any appropriate or necessary updates in good faith, including the addition, amendment, or replacement of any Addenda.

4. ROLES AND SCOPE OF PROCESSING

4.1. **Customer Processing of Personal Information.** Customer: (i) agrees that it will comply with its obligations under Data Protection Laws in respect of its Processing of Personal Information and any Processing instructions it issues to WSP; and (ii) represents and warrants that it has provided all fair processing notices and obtained all consents and rights necessary under Data Protection Laws for WSP to Process Customer Personal Information and provide the WSP Offerings pursuant to the Agreement and this DPA.

4.2. **Customer Instructions.** WSP will Process Customer Personal Information only for the purposes described in the Agreement and only in accordance with Customer's documented lawful instructions and applicable Data Protection Laws. WSP will not Process Customer Personal Information provided by or collected on behalf of Customer for any purpose except as necessary to maintain or provide the WSP Offerings specified in the Agreement and this DPA, or as necessary to comply with the law or binding order of a governmental body. In the event that WSP has a legal obligation to Process the Customer Personal Information, WSP will notify the Customer of this obligation unless it is legally prohibited from doing so. The parties agree that this DPA and the Agreement set out the Customer's complete instructions to WSP in relation to the Processing of Customer Personal Information by WSP. Additional Processing outside the scope of these instructions (if any) will require prior written agreement between Customer and WSP.

4.3. **Data Processing Specifications.** Attached to this DPA are the details of the Processing as Schedule D.

4.4. **Customer Personal Information for Support.** Customer acknowledges that WSP does not ordinarily require the Processing of Customer Personal Information on Customer's behalf to resolve a technical issue for Support. Customer shall use commercially reasonable efforts to minimize any transfer of Customer Personal Information to WSP for Support purposes. Such efforts shall include, but not be limited to, removing, anonymizing and/or pseudonymizing Customer Personal Information in files submitted to WSP in a Support request prior to any Processing by WSP, in each case to the extent such removal, anonymization and/or pseudonymization is reasonably practicable under the circumstances.

5. SUB-PROCESSING

5.1. **Authorised Sub-processors.** Customer understands and hereby authorises WSP to engage Subprocessors to Process Customer Personal Information on Customer's behalf as identified in Schedule D.

5.2. **Sub-processor obligations.** WSP will: (i) not engage a Sub-processor unless WSP enters into a written agreement with the Sub-processor which contains obligations that are at least as restrictive as those set out in this DPA; and (ii) remain responsible for the performance of its obligations under this DPA, including the performance of the obligations by the Sub-processor.

6. SECURITY

6.1. **Security Measures.** Taking into account the nature of the Processing, WSP shall implement and maintain reasonable technical and organisational security measures to protect Customer Personal Information from Security Incidents and to preserve the security and confidentiality of the Customer Personal Information, in accordance with WSP's security standards described in Schedule A, as applicable to the (SaaS) Services ("Security Measures").

6.2. **Updates to Security Measures.** Customer is responsible for reviewing the information made available by WSP relating to the Security Measures and making an independent determination as to whether such Security Measures meet Customer's requirements and legal obligations under Data Protection Laws. Customer acknowledges that the Security Measures are subject to technical progress and development and that WSP may update or modify the Security Measures from time-to-time provided that such updates and modifications do not result in a material degradation of the overall security of the WSP Offerings.

6.3. **Customer Responsibilities.** Customer agrees that, without prejudice to WSP's obligations under Section 6.1 (Security Measures) and Section 9.2 (Security Incident Response):

A. Customer is responsible for its use of the WSP Offerings, including: (i) making appropriate use of the WSP Offerings to ensure a level of security appropriate to the risk in respect of the Customer Personal Information;(ii) securing its account authentication credentials; (iii) protecting the security of Customer Personal Information when in transit to and from the WSP Offerings; (iv) taking appropriate steps to securely encrypt and/or backup any Customer Personal Information uploaded to the WSP Offerings; and (v) properly configuring the WSP Offerings and using available features and functionalities to maintain appropriate security in light of the nature of the Customer Personal Information Processed as a result of Customer's use of the WSP Offerings; and

B. WSP has no obligation to protect Customer Personal Information that Customer elects to store or transfer outside of WSP's and its Sub-processors' (where applicable) systems (for example, offline or on-premises storage).

7. SECURITY REPORTS AND AUDITS

7.1. Upon request, WSP shall provide to Customer (on a confidential basis) a summary copy of any third party audit report(s) or certifications applicable to the WSP Offerings ("Report"), so that Customer can verify WSP's compliance with this DPA, the audit standards against which it has been assessed, and the standards specified in the WSP Security Measures, as described in Schedule A.

7.2. If Customer reasonably believes that the Report provided is insufficient to demonstrate compliance with this DPA, WSP shall also provide written responses (on a confidential basis) to reasonable requests for information made by Customer related to its Processing of Customer Personal Information, including responses to information security and audit questionnaires that are reasonably necessary to demonstrate WSP's compliance with this DPA, provided that Customer shall not be permitted to exercise this right more than once every 12 months.

7.3. If Customer reasonably believes that the information provided pursuant to Sections 7.1 and/or 7.2 is insufficient to demonstrate compliance with this DPA, WSP will allow an audit by Customer (or auditors appointed by Customer and reasonably acceptable to WSP) in relation to WSP's Processing of Customer Personal Information. Any such audit will be at Customer's expense, with reasonable advance notice, conducted during normal business hours, carried out no more than once every 12 months and subject to WSP's reasonable security and confidentiality requirements, provided that the exercise of rights under this Section would not infringe Data Protection Laws.

8. INTERNATIONAL OPERATIONS.

8.1. WSP may store and Process Customer Personal Information in any countries where WSP, its Affiliates or its Sub-processors maintain data processing operations. The Sub-processors are identified in Schedule D (as may be amended from time to time).

9. ADDITIONAL SECURITY

9.1. **Confidentiality of Processing.** WSP shall ensure that any person who is authorised by WSP to Process Customer Personal Information (including its staff, agents and subcontractors) shall be under an appropriate obligation of confidentiality (whether a contractual or statutory duty).

9.2. **Security Incident Response.** WSP shall: (i) taking into account the nature of WSP's Processing of Customer Personal Information and the information available to WSP, notify Customer of a Security Incident that it becomes aware of, without undue delay; (ii) provide timely information relating to the Security Incident as it becomes known or as is reasonably requested by Customer; and (iii) promptly take reasonable steps to contain, investigate, and mitigate any Security Incident.

9.3. **Notification.** Customer acknowledges that WSP will not assess the contents of Customer Personal Information in order to identify information subject to any specific legal requirements. Customer is solely responsible to comply with incident notification laws applicable to Customer and fulfilling any third-party notification obligations related to any Security Incidents as required by Data Protection Laws. Unless otherwise required under Data Protection Laws, the parties agree to coordinate in good faith on developing

the content of any related public statements or any required notices for the affected data subjects and/or notices to the relevant supervisory authorities.

10. RELATIONSHIP WITH THE AGREEMENT

10.1. Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. If there is any conflict between this DPA and the Agreement, this DPA shall prevail to the extent of that conflict in connection with the Processing of Customer Personal Information.

10.2. Notwithstanding anything to the contrary in the Agreement or this DPA, the liability of each party and each party's Affiliates under this DPA shall be subject to the exclusions and limitations of liability set out in the Agreement. Without limiting either of the parties' obligations under the Agreement, Customer agrees that any regulatory penalties incurred by WSP that arise as a result of, or in connection with, Customer's failure to comply with its obligations under this DPA or any applicable Data Protection Laws shall count toward and reduce WSP's liability under the Agreement as if it were liability to the Customer under the Agreement.

10.3. Any claims against WSP or its Affiliates under this DPA shall only be brought by the Customer entity that is a party to the Agreement against the WSP entity that is a party to the Agreement. In no event shall this DPA or any party to this DPA restrict or limit the rights of any data subject or of any competent supervisory authority.

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

10.5. This DPA will run co-terminus with the Agreement and terminate automatically with the termination or expiry of the Agreement, subject to additional provisions in any Addenda attached hereto.

***

SCHEDULE A – SECURITY MEASURES WSP GROUP DATA SECURITY PROGRAM

WSP has implemented and shall maintain a commercially reasonable security program in accordance with industry best practices, which shall include technical and organisational measures to ensure an appropriate level of security for Customer Personal Information taking into account the risks presented by the Processing, in particular from accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of, or access to Customer Personal Information, and the nature of the Customer Personal Information to be protected having regard to the state of the art and the cost of implementation. WSP's security program shall include the following measures:

1. **Security Program**

   a. **ISO27001-based Information Security Management System (ISMS)**: WSP shall maintain an ISMS risk-based security program to systematically manage and protect the organisations' business information and the information of its customers and partners.

   b. **Security Governance Committee**: WSP shall maintain a security committee comprised of leaders across all business units that oversees the company's security program. This committee shall meet monthly to review the operational status of the ISMS (including risks, threats, remediation actions, and other security-related issues) and drive continuous security improvement throughout the business.

   c. **Security incident response policy**: WSP shall maintain policies and procedures to (1) investigate and respond to security incidents, including procedures to assess the threat of relevant vulnerabilities or security incidents using defined incident classifications and categorisations and (2) establish remediation and mitigation actions for events, including artifact and evidence collection procedures and defined remediation steps.

   d. **Policy maintenance**: All security and privacy related policies shall be documented, reviewed, updated and approved by management at least annually to ensure they remain consistent with best practices, legal and regulatory requirements and industry standards.

   e. **Communication and commitment**: Security and privacy policies and procedures shall be published and effectively communicated to all personnel and relevant subcontractors. Security shall be addressed at the highest levels of the company with executive management regularly discussing security issues and leading company-wide security initiatives.

2. **Personnel Security**

   a. **Background screening**: Personnel who have access to Customer Personal Information or the equipment on which it is stored shall be subject to background screening (as allowed by local laws and regulations) that shall include verification of identity, right to work and academic degrees and a check of criminal records, sex offender registries and prohibited/denied party lists.

   b. **Confidentiality obligations**: Personnel who have access to Customer Personal Information shall be subject to a binding contractual obligation with WSP to keep the Customer Personal Information confidential.

   c. **Security awareness training**: Personnel shall receive training upon hire and at least annually thereafter covering security best practices and privacy principles.

   d. **Code of conduct**: WSP shall maintain a code of business conduct policy and compliance program to ensure ethical behavior and compliance with applicable laws and regulations.

3. **Third-Party Security**

   a. **Screening**: WSP shall maintain policies and procedures to ensure that all new suppliers, SaaS applications, IT Software, and IT service solutions are subject to reasonable due diligence to confirm their ability to meet corporate security and compliance requirements as well as business objectives.

   b. **Contractual obligations**: WSP shall ensure that contractual agreements with suppliers include confidentiality and privacy provisions as appropriate to protect WSP's interests and to ensure WSP can meet its security and privacy obligations to customers, partners, employees, regulators and other stakeholders.

c. **Monitoring**: WSP shall periodically review existing third-party suppliers to ensure the supplier complies with contractual terms, including any security and availability requirements. The monitoring program shall review suppliers at least annually (regardless of length of contractual term) to confirm that the supplier/solution is still meeting the company's objectives and the supplier's performance, security, and compliance postures are still appropriate given the type of access and classification of data being accessed, controls necessary to protect data, and applicable legal and regulatory requirements.

4. **Physical Security**

a. **Corporate facility security**: A facility security program shall be maintained that manages building entrances, CCTVs, and overall security of its offices, including a security perimeter (including barriers such as card controller entry gates or manned reception desks).

b. **Corporate data center security**: Systems used to Process Customer Personal Information shall be protected in such a manner that unauthorised logical or physical access is effectively prevented; equipment used to Process Customer Personal Information cannot be moved, removed, upgraded or reconfigured without appropriate authorisation and protection of the information; and, when equipment Processing Customer Personal Information is decommissioned, Customer Personal Information shall be disposed of securely in a manner that would prevent its reconstruction.

c. **SaaS Services data center security**: WSP leverages Infrastructure as a Service (IaaS) data centers for hosting the SaaS Services. WSP assesses the security and compliance measures of the applicable data center providers, and the providers follow industry best practices and comply with numerous standards.

5. **Solution Security**

a. **Software development life cycle (SDLC)**: WSP shall maintain a software development life cycle policy that defines the process by which personnel create secure products and services and the activities that personnel must perform at various stages of development (requirements, design, implementation, verification, documentation and delivery).

b. **Secure development**: Product management, development, test and deployment teams shall follow secure application development policies and procedures that are aligned to industry-standard practices, such as the OWASP Top 10.

c. **Vulnerability assessment**: WSP shall regularly conduct risk assessments, vulnerability scans and audits (including third-party penetration testing of the SaaS Services twice annually and software upon each new version release). Identified product solution issues shall be scored using the Common Vulnerability Scoring System (CVSS) risk-scoring methodology based on risk impact level and the likelihood and potential consequences of an issue occurring. Vulnerabilities are remediated on the basis of assessed risk. Upon request from Customer, WSP shall provide information about the identified vulnerabilities and the measures taken to remediate or address any such vulnerabilities.

6. **Operational Security**

a. **Access controls**: WSP shall maintain policies, procedures, and logical controls to establish access authorisations for employees and third parties to limit access to properly authorised personnel and to prevent unauthorised access. Such controls shall include:

i. requiring unique user IDs to identify any user who accesses systems or data;

ii. managing privileged access credentials in a privileged account management (PAM) system;

iii. communicating passwords separately from user IDs;

iv. ensuring that user passwords are (1) changed at regular intervals; (2) of sufficient length and complexity; (3) stored in an encrypted format; (4) subject to reuse limitations; and (5) not assigned to other users, even at a different time; and

v. automatically locking out users' IDs when a number of erroneous passwords have been entered.

b. **Least privilege**: WSP shall ensure that personnel only have access to systems and data as required for the performance of their roles; only authorised personnel have physical access to infrastructure and equipment; access to production resources for the SaaS Services is restricted to employees requiring access; and access rights are reviewed and certified at least annually to ensure access is appropriate.

c. **Malware**: WSP shall utilise industry-standard measures to detect and remediate malware, viruses, ransomware, spyware, and other intentionally harmful programs that may be used to gain unauthorised access to information or systems.

d. **Encryption**: WSP shall use industry-standard strong encryption methods to protect data in transit and at rest as appropriate to the sensitivity of the data and the risks associated with loss; all laptops and other removable media, including backup tapes, on which Customer Personal Information is stored shall be encrypted.

e. **Business continuity and disaster recovery (BCDR)**: WSP shall maintain formal BCDR plans that are regularly reviewed and updated to ensure WSP's systems and services remain resilient in the event of a failure, including natural disasters or system failures.

f. **Data backups**: WSP shall backup data and systems using alternative site storage available for restore in case of failure of the primary system. All backups shall use strong encryption in transit and at rest.

g. **Change management**: WSP shall maintain change management policies and procedures to plan, test, schedule, communicate, and execute changes to WSP's SaaS Services infrastructure, systems, networks, and applications.

h. **Network security**: WSP shall implement industry standard technologies and controls to protect network security, including firewalls, intrusion prevention systems, monitoring, network segmentation, VPN and wireless security. Networks shall be designed and configured to restrict connections between trusted and untrusted networks, and network designs and controls shall be reviewed at least annually.

i. **Data segregation**: WSP shall implement logical controls, including logical separation, access controls and encryption, to segregate Customer's Personal Information from other customer and WSP data in the SaaS Services. WSP shall additionally ensure that production and nonproduction data and systems are separated.

SCHEDULE B – EUROPEAN ADDENDUM

This European Addendum ("European Addendum") supplements the DPA and includes additional information required by European Data Protection Law (as defined below). All words or phrases used herein not defined in this European Addendum will have the meaning assigned to them in the DPA and/or the Agreement.

1. Scope

This European Addendum shall apply in the event that: (i) WSP Processes Customer Personal Information on the behalf of Customer as a Processor in the course of providing WSP Offerings pursuant to the Agreement; and (ii) WSP is subject to European Data Protection Law and acts as a Processor thereunder and/or Customer is subject to European Data Protection Law and act as a Controller thereunder.

2. Definitions

2.1 "**EEA**" means, for the purposes of this DPA, the European Economic Area.

2.2 "**European Data Protection Law**" means: (i) the Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ("GDPR") as implemented by countries within the EEA; (ii) the European Union e-Privacy Directive 2002/58/EC as implemented by countries within the EEA; (iii) to the extent that WSP Processes any Personal Information subject to the data protection laws in the United Kingdom of Great Britain and Northern Ireland (collectively, the "UK"), all laws relating to data protection, the processing of personal information, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR (as defined in section 3 of the Data Protection Act 2018) and the Data Protection Act 2018 (collectively "UK Privacy Law"); (iv) to the extent that WSP Processes any Personal Information subject to the data protection laws in Switzerland, the Swiss Federal Act on Data Protection ("FADP"); and/or (v) other laws that are similar, equivalent to, successors to, or that are intended to or implement the laws that are identified in (i), (ii), (iii), and (iv) above.

2.3 "**SCCs**" means, collectively, (i) where Personal Information of data subjects in the EEA is involved, the Standard Contractual Clauses as approved by the European Commission in the form set out in Commission Implementing Decision (EU)2021/914 of 4 June 2021 for the transfer of personal data to third countries pursuant to GDPR ("EU SCCs"), and (ii) where Personal Information of data subjects in the UK is involved, the EU SCCs as amended by the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner under Section 119A(1) Data Protection Act 2018 ("UK SCCs"), in each case, as completed as described in Section 5 below.

2.4 All terms used herein not defined in the DPA will have the meaning assigned to them in the applicable European Data Protection Law. All references to Data Protection Law or laws in the DPA shall be read in the context of EU or Member State law for the purpose of this Addendum.

3. Sub-processors.

3.1 WSP's Sub-processors Are identified in Schedule D (as may be amended from time to time).

3.2 To the extent that WSP Processes any Customer Personal Information from the EEA, the UK, or Switzerland, and provides such Customer Personal Information to another party (including Affiliates and/or Sub-processors) outside of the EEA, the UK, or Switzerland in countries not deemed by the European Commission, the UK Information Commissioner's Office, or Switzerland to provide an adequate level of data protection, WSP will (as "data exporter") transfer the Customer Personal Information to the third party (as "data importer") in compliance with chapter V of the GDPR, by, for instance, adopting the appropriate set and module of the SCCs.

3.3 For the engagement of Sub-processors by WSP under this European Addendum the following applies:

(a) WSP shall notify Customer, in writing, of any intended additional or replacement Sub-processor who will Process Customer Personal Information at least thirty (30) days prior to when the Subprocessor begins Processing Customer Personal Information (such period, the "**Review Period**");

(b) Customer may object to any additional or replacement Sub-processor at any time during the Review Period. Any objections raised by Customer during the Review Period may only be based on reasonable grounds and only with respect to data protection concerns;

(c) Customer may object to WSP's additional or replacement Sub-processor by providing notice of Customer's objection, in writing, and in the manner provided in the Agreement. WSP will have a reasonable time to notify Customer, in writing, that the proposed addition or replacement shall not apply to any of the WSP Offerings provided by WSP to the Customer or allow the Customer to terminate for convenience the affected WSP Offerings used by Customer, and in the manner provided in the Agreement. Customer will continue to pay all fees for the affected WSP Offerings until the termination takes effect, and WSP will refund Customer on a pro-rated basis any unused and prepaid fees covering the remainder of the term of the terminated Agreement following the effective date of termination; and

(d) The parties agree that any non-response by the Customer during the Review Period will be taken as the Customer's approval of additional or replacement Sub-processors, where Customer continues to use the WSP Offerings after the Review Period has lapsed. CLAUSE 9(A) OF THE SCCS AND THIS SECTION 3.3 STATE THE ENTIRE LIABILITY OF WSP AND THE SOLE REMEDY FOR CUSTOMER IN CONNECTION WITH ANY OBJECTION BY CUSTOMER TO AN INTENDED ADDITIONAL OR REPLACEMENT SUB-PROCESSOR WHO WILL PROCESS CUSTOMER PERSONAL INFORMATION.

4. Cooperation

4.1 Taking into account the nature of the Processing, WSP shall (at Customer's request, cost, and expense) provide reasonable cooperation to assist Customer to respond to any requests from data subjects in relation to their data subject rights under European Data Protection Laws or applicable regulatory authorities relating to the Processing of Customer Personal Information under the Agreement.

4.2 If a law enforcement agency sends WSP a demand for Customer Personal Information (e.g., a subpoena or court order), WSP will attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, WSP may provide Customer's contact information to the law enforcement agency. If compelled to disclose Customer Personal Information to a law enforcement agency, then WSP will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy to the extent WSP is legally permitted to do so.

4.3 In the event that any request from data subjects or applicable regulatory authorities is made directly to WSP, WSP shall not respond to such communication directly without Customer's prior authorisation other than to inform the requestor that WSP is not authorised to directly respond to a request, and recommend the requestor submit the request directly to Customer, unless legally compelled to reply. Customer shall bear the responsibility for responding to all such requests.

4.4 If WSP is legally required to respond to a request enumerated in Sections 4.2 and 4.3, WSP will promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so.

4.5 Customer acknowledges that WSP may be required under European Data Protection Law to: (i) collect and maintain records of certain information, including the name and contact details of each Processor and/or Controller on behalf of which WSP is acting and, where applicable, of such Processor's or Controller's local representative and data protection officer; and (ii) make such information available to the supervisory authorities. Accordingly, if European Data Protection Law applies to the Processing of Customer Personal Information, Customer will, where requested, provide such information to WSP, and will ensure that all information provided is kept accurate and up-to-date.

4.6 Taking into account the nature of the Processing and information available to WSP, WSP shall (at Customer's request and expense) provide reasonably requested information regarding the WSP Offerings to enable the Customer to carry out data protection impact assessments.

4.7 Upon Customer's written request and after the termination of the Agreement and this DPA, WSP shall delete or return all Customer Personal Information, unless retention of such Customer Personal Information is required by law (including as reflected in WSP data retention policies) or the Agreement.

5. Standard Contractual Clauses

5.1 To the extent that WSP Processes any Customer Personal Information from the EEA, the UK, or Switzerland, and receives such Customer Personal Information outside of the EEA, the UK, or Switzerland in countries not deemed by the European Commission, the UK Information Commissioner's Office, or Switzerland to provide an adequate level of data protection ("**Restricted Transfers**"), the SCCs will apply to any Restricted Transfers from Customer and Customer Affiliates (each as "data exporter") to WSP (as "data importer") as follows:

(a) **EU Personal Information**. In respect of Customer Personal Information that is protected by the EU GDPR, the EU SCCs will apply for any Restricted Transfers, are incorporated by reference, and are completed as follows:

(i) Module 2 applies;

(ii) in Clause 7, the optional docking clause will apply;

(iii) in Clause 9, Option 2 will apply, and will be completed and subject to Section 3 (Subprocessors) of the European Addendum;

(iv) in Clause 11, the optional redress language will not apply;

(v) in Clause 17, Option 2 will apply, and the EU SCCs will be governed by the law specified in the Agreement, provided that law is an EU Member State law recognizing third party beneficiary rights, otherwise, the laws of the applicable supervisory authority determined under Clause 13 of the EU SCCs shall govern;

(vi) in Clause 18(b), disputes shall be resolved before the courts specified in the Agreement, provided these courts are located in an EU Member State, otherwise those courts shall be the courts of the EU Member State of the applicable supervisory authority determined under Clause 13 of the EU SCCs; and

(vii) in all cases the parties satisfy any signature requirement in "Annex 1: List of Parties" to the EU SCCs by the execution or acceptance of Customer and WSP to the binding Agreement effective between the parties.

(b) **UK Personal Information**. In respect of Personal Information that is protected by the UK Privacy Law, the UK SCCs will apply for any Restricted Transfers, are incorporated by reference, and are completed as follows:

(i) Table 1 of the UK SCCs is completed with the relevant information in Section 5.1(d) of the European Addendum;

(ii) Table 2 of the UK SCCs is completed with the selected modules and clauses from the EU SCCs as identified in Section 5.1(a) of the European Addendum;

(iii) Table 3 of the UK SCCs is completed with the relevant information in Sections 5.1(d) and 5.1(e) of the European Addendum;

(iv) both the importer and the exporter may terminate the UK SCCs in Table 4 of the UK SCCs in accordance with the terms of the UK SCCs; and

(v) in all cases the parties satisfy any signature requirement in UK SCCs by the execution or acceptance of Customer and WSP to the binding Agreement effective between the parties.

(c) **Swiss Personal Information**. In respect of Personal Information that is protected by the FADP, the EU SCCs as completed in Section 5.1(a) will apply for any Restricted Transfers, are incorporated by reference, and are amended as follows:

(i) the term "personal data" or "personal information" shall be deemed to include information relating to an identified or identifiable legal entity;

(ii) references to (articles in) the EU General Data Protection Regulation 2016/679 shall be deemed to refer to (respective articles in) the FADP;

(iii) reference to the competent supervisory authority in Annex I. C. under Clause 13 of the SCCs shall be deemed to refer to the Federal Data Protection and Information Commissioner ("**FDPIC**");

(iv) references to Member State(s)/EU Member State(s) shall be deemed to include Switzerland;

(v) reference to the European Union in Annex I (A) shall be deemed to include Switzerland;

(vi) where the Clauses use terms that are defined in the GDPR, those terms shall be deemed to have the meaning as the equivalent terms are defined in the FADP;

(vii) the list of data subjects and categories of data indicated in Annex I. B. to the SCCs shall not be deemed to restrict the application of the SCCs to the Swiss Personal Information; and

(viii) in all cases the parties satisfy any signature requirement under the FADP by the execution or acceptance of Customer and WSP to the binding Agreement effective between the parties.

(d) **SCC Annex I:**

(i) In respect of Annex I, Section A of the EU SCCs, the requisite information is as follows:

(A) Data exporter(s):

Name: as identified in the Agreement
Address: as identified in the Agreement
Contact person's name, position and contact details: as identified in the Agreement
Activities relevant to the data transferred under these Clauses: For any on-premises software: WSP's Support and Other Services (e.g., program planning, software deployment assistance, interface adapter efforts, and/or formal or nonformal software training).
For any SaaS solutions: WSP's SaaS Services, Support, and Other Services (e.g., implementation services, implementation support, best practices consultations, integration efforts, and training and education services).
Signature and date: the parties agree that any signature requirement is satisfied by the execution or acceptance of Customer and WSP to the binding Agreement effective between the parties.
Role (controller/processor): Controller

(B) Data importer(s):

Name: WSP
Address: as identified in the Agreement
Contact person's name, position and contact details: as identified in the Agreement.
Activities relevant to the data transferred under these Clauses:
Same as listed above for data exporter.
Signature and date: the parties agree that any signature requirement is satisfied by the execution or acceptance of Customer and WSP to the binding Agreement effective between the parties.

Role (controller/processor): Processor

(ii) In respect of Annex I, Section B of the EU SCCs, the requisite information is as follows:

(A) Please see Section 4.3 (Details of Data Processing) of the DPA for details of transfer(s);

(B) For transfers to (sub-) processors,

(I) Subject matter of sub-processing:

Identification and contact data (e.g., name, address, title, contact details), employment details (e.g., job title, role, manager), and/or IT information (e.g., entitlements, IP addresses, usage data, cookies data, and geolocation) for Customer's employees, contractors, and/or (where licensed under the Agreement) data exporter's business partners and/or end-users authorised by Customer.

(II) Nature of sub-processing:

To assist WSP in providing WSP Offerings to Customer under the Agreement.

(III) Duration of sub-processing:

The sub-processing will occur for the duration of the processing by WSP in the context of the provision of WSP Offerings under the Agreement unless WSP earlier terminates and/or replaces the subprocessor.

(iii) In respect of Annex I, Section C of the EU SCCs, the competent supervisory authority shall be the applicable supervisory authority determined under Clause 13 of the EU SCCs.

(e) **SCC Annex II:**

(i) In respect of Annex II of the EU SCCs, the requisite information is as follows:

(A) Description of the technical and organisational measures implemented by the data importer(s)

(I) Application to Transfers

Cross-border transfers by Customer to WSP relate to WSP's (1) Support Services for Products and/or (2) Professional Services. Customer controls what data WSP has access to for these purposes. As such, WSP's technical and organisational measures, as a whole, concern its access to transferred data.

(II) Technical and Organisational Measures

Please see Schedule A of the DPA, which describes the technical and organisational security measures implemented by WSP.

(B) For transfers to (sub-) processors, Sub-processors shall ensure that they have appropriate technical and organisational measures to protect against and report a personal data breach, appropriate to the harm that might result from such personal data breach, having regard to the state of technological development and the cost of implementing any measures. Such measures may include where appropriate: pseudonymising or encrypting personal data, ensuring confidentiality, integrity, availability and resilience of its systems and services, ensuring that availability of and access to personal data can be restored in a

timely manner after a physical or technical incident, and regularly assessing and evaluating the effectiveness of the technical and organisational measures adopted by it.

5.2 The parties agree that the data export solution identified in Section 5.1 (Standard Contractual Clauses) will not apply if and to the extent that WSP adopts an alternative data export solution for the lawful transfer of Personal Information (as recognised under European Data Protection Laws) outside of the EEA, the UK, or Switzerland in which event, Customer shall take any action (which may include execution of documents) required to give effect to such solution and the alternative transfer mechanism will apply instead (but only to the extent such alternative transfer mechanism extends to the jurisdictions to which Customer Personal Information is transferred).

SCHEDULE C - UNITED STATES PRIVACY LAW ADDENDUM

This United States Privacy Law Addendum ("US Addendum") supplements the DPA and includes additional information required by the CPRA and VCDPA (each as defined below). All words or phrases used herein not defined in this US Addendum will have the meaning assigned to them in the DPA and/or the Agreement.

1. CALIFORNIA

1.1 Scope

(a) This Section 1 shall apply in the event that WSP Processes Customer Personal Information of California residents.

1.2 Definitions

(a) The California Consumer Privacy Act is Cal. Civ. Code § 1798.100, et seq. as amended by the California Privacy Rights Act ("CPRA"), as may be amended from time-to-time, and any accompanying legally binding regulations that are promulgated to address provisions in the CPRA.

(b) For purposes of this Section 1, the terms "Business," "Business Purpose," "Commercial Purpose," "Consumer," "Personal Information," "Processing," "Sell," "Service Provider," "Share," and "Verifiable Consumer Request" shall have the meanings set forth in the CPRA.

(c) All references to "Personal Information," "Controller," "Processor," and "Data Subject" in the DPA shall be deemed to be references to "Personal Information," "Business," "Service Provider," and "Consumer" as defined in the CPRA.

1.3 Terms

(a) The parties acknowledge and agree that Customer is a Business and WSP is a Service Provider for the purposes of the CPRA (to the extent it applies) and WSP is receiving Personal Information from Customer in order to provide the WSP Offerings pursuant to the Agreement, which constitutes a Business Purpose.

(b) Customer will disclose Personal Information to WSP only for the limited and specified purposes described in Section 4.3 of the DPA.

(c) WSP will not Sell or Share Personal Information provided by Customer under the Agreement.

(d) WSP will not retain, use, or disclose Customer Personal Information provided by Customer pursuant to the Agreement for any purpose, including a Commercial Purpose, other than as necessary for the specific purpose of providing the WSP Offerings for Customer pursuant to the Agreement, or as otherwise set forth in the Agreement or as permitted by the CPRA.

(e) WSP will not retain, use, or disclose Personal Information provided by Customer pursuant to the Agreement outside of the direct business relationship between WSP and Customer, except where and to the extent permitted by the CPRA.

(f) WSP will notify Customer if it makes a determination that it can no longer meet its obligations under the CPRA.

(g) Except and to the extent permitted by the CPRA, WSP will not combine Personal Information received from, or on behalf of, Customer with Personal Information that it receives from, or on behalf of, another party, or that it collects from its own interaction with the Consumer.

(h) WSP will comply with all obligations applicable to Service Providers under the CPRA, including by providing Personal Information provided by Customer under the Agreement the same level of privacy protection required by CPRA.

(i) In the event that WSP engages a new Sub-processor to assist WSP in providing the WSP Offerings to Customer under the Agreement, WSP will (i) notify Customer, in writing, of any intended additional or replacement Sub-processor who will Process Customer Personal Information at least thirty (30) days prior to when the Sub-processor begins Processing

Customer Personal Information; and (ii) enter into a written contract with the Sub-processor requiring Sub-processor to observe all of the applicable requirements set forth in the CPRA.

1.4 Consumer Rights

(a) Taking into account the nature of the Processing, WSP shall (at Customer's request and expense) provide reasonable cooperation to assist Customer to respond to Verifiable Consumer Requests to exercise the Consumer's rights under the CPRA, where possible, provided that (i) Customer is itself unable to respond without WSP's assistance and (ii) WSP is able to do so in accordance with all applicable laws, rules, and regulations. In the event that any request from consumers or applicable regulatory authorities is made directly to WSP, WSP will not respond to such communication directly without Customer's prior authorisation other than to inform the requestor that WSP is not authorised to directly respond to a request, and recommend the requestor submit the request directly to Customer, unless legally compelled to do so, and instead, after being notified by WSP, Customer will respond. If WSP is required to respond to such a request, WSP will promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so. Customer is solely responsible for ensuring that Consumer requests are communicated to WSP, and, if applicable, for ensuring that a record of consent to processing is maintained with respect to each Consumer.

(b) If a law enforcement agency sends WSP a demand for Customer Personal Information (e.g., a subpoena or court order), WSP will attempt to redirect the law enforcement agency to request that data directly from Customer. As part of this effort, WSP may provide Customer's contact information to the law enforcement agency. If compelled to disclose Customer Personal Information to a law enforcement agency, then WSP will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy to the extent WSP is legally permitted to do so.

1.5 Audit Rights

(a) To the extent required by the CPRA, WSP will allow Customer to conduct inspections or audits in accordance with Section 7 of the DPA.

2. <u>VIRGINIA</u>

2.1 Scope

(a) This Section 2 shall apply in the event that WSP Processes Customer Personal Information of Virginia residents.

2.2 Definitions

(a) The Virginia Consumer Data Protection Act is Va. Code §§ 59.1-575 et seq. ("VCDPA"), as may be amended from time-to-time, and any accompanying legally binding regulations that are promulgated to address provisions in the law.

(b) For purposes of this Section 2, the terms "Consumer," "Controller," "Personal Data," "Processing," and "Processor" shall have the meanings set forth in the VCDPA.

(c) For purposes of this Section 2, all references to "Data Subject" in this DPA shall be deemed to be references to "Consumer" as defined in the VCDPA.

2.3 Obligations

(a) The parties acknowledge and agree that Customer is a Controller and WSP is a Processor for the purposes of the VCDPA (to extent it applies).

(b) The nature, purpose, and duration of Processing, as well as the types of Personal Data and categories of Consumers are described in Section 4.3 of the DPA.

(c) WSP shall adhere to Customer's instructions with respect to the Processing of Customer Personal Data and shall assist Customer in meeting its obligations under the VCDPA by:

(i) taking into account the nature of the Processing, at Customer's request and expense, providing reasonable cooperation to assist Customer to respond to Consumer rights requests where possible, provided that (i) Customer is itself unable to respond without WSP's assistance and (ii) WSP is able to do so in accordance with all applicable laws, rules, and regulations. In the event that any request from consumers or applicable regulatory authorities is made directly to WSP, WSP will not respond to such communication directly without Customer's prior authorisation other than to inform the requestor that WSP is not authorised to directly respond to a request, and recommend the requestor submit the request directly to Customer, unless legally compelled to do so, and instead, after being

notified by WSP, Customer will respond. If WSP is required to respond to such a request, WSP will promptly notify Customer and provide it with a copy of the request unless legally prohibited from doing so. Customer is solely responsible for ensuring that Consumer requests are communicated to WSP, and, if applicable, for ensuring that a record of consent to processing is maintained with respect to each Consumer.

(ii) Complying with Section 6 ("Security") of the DPA with respect to Personal Data provided by Customer;

(iii) In the event of a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to Personal Data, providing information sufficient to enable Customer to meet its obligations pursuant to Va. Code § 18.2186.6; and

(iv) Providing information sufficient to enable Customer to conduct and document data protection assessments to the extent required by VCDPA.

(d) WSP shall maintain the confidentiality of Personal Data provided by Customer and require that each person Processing such Personal Data be subject to a duty of confidentiality with respect to such Processing;

(e) Upon Customer's written request, WSP shall delete or return all Personal Data provided by Customer, unless retention of such Personal Data is required or authorised by law or the DPA and/or Agreement.

(f) In the event that WSP engages any new Sub-processor to assist WSP in providing the WSP Offerings to Customer under the Agreement, WSP shall enter into a written contract with the Sub-processor requiring Sub-processor to observe all of the applicable requirements of a Processor set forth in the VCDPA.

2.4 Audit Rights

(a) Upon Customer's written request at reasonable intervals, WSP shall, as set forth in Section 7 of the DPA, (i) make available to Customer all information in its possession that is reasonably necessary to demonstrate WSP's compliance with its obligations under the VCDPA; and (ii) allow and cooperate with reasonable inspections or audits as required under the VCDPA.

SCHEDULE D – DATA PROCESSING SPECIFICATIONS

Depending on the WSP Offerings identified in the Order, the following describes the Processing of Personal Information:

Processing of personal information

(a) Categories of data subjects whose Personal Information is transferred:

Customer's employees, contractors, and/or (where licensed under the Agreement) data exporter's business partners and/or end-users authorised by Customer.

(b) Categories of Personal Information transferred:

Identification and contact data (e.g., name, address, title, contact details), employment details (e.g., job title, role, manager), and/or IT information (e.g., entitlements, IP addresses, usage data, cookies data, and geolocation), and, if applicable, the Personal Information as described in the table hereunder.

(c) Sensitive data transferred (if applicable):

None.

(d) The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)

***For Professional Services: one-off**. Customer controls what information (including Personal Information) it shares with WSP and when it shares such information (including Personal Information) in the context of the provision of Professional Services under the Agreement.*

***For SaaS and Support Services: continuous**. Customer controls what information (including Personal Information) it shares with WSP and what systems it connects to the SaaS Services and Support Services. The SaaS Services may allow for a one-off data transfer or connectivity to facilitate transfer on a regularly scheduled and/or continuous basis. Customer determines its configuration and use of the SaaS Services under the Agreement*.

(e) Nature of the processing

To provide WSP Offerings to Customer under the Agreement.

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

The provision of WSP Offerings by WSP under the Agreement.

(g) The period for which the Personal Information will be retained, or, if that is not possible, the criteria used to determine that period.

The Customer Personal Information Processed by WSP will be retained for the duration of the Processing by WSP in the context of the provision of WSP Offerings under the Agreement, and thereafter in order to comply with applicable law, including Data Protection Laws. Should the Customer make a request to have continued access to its Customer Personal Information, WSP will, after a recovery period of up to 30 days following such expiry or termination, comply with this instruction as soon as reasonably practicable, where technically feasible. Customer shall be responsible for retrieving any remaining Customer Personal Information it wishes to retain before the end of the recovery period. WSP shall not be required to delete or return Customer Personal Information to the extent: (i) WSP is required by applicable law or order of a governmental or regulatory body to retain some or all of the Customer Personal Information; and/or (ii), Customer Personal Information it has archived on back-up systems, which Customer Personal Information WSP shall securely isolate and protect from any further processing, except to the extent required by applicable law.

(h) The locations of processing operations.

The SaaS Services are available from three main Microsoft Azure Regions. Besides EMEA, there is regional presence in the Americas and Asia-Pacific region.

Region	Sub region	Physical location
EMEA	Germany West Central	Frankfurt
APAC	Australia East	New South Wales

NORA	Central US	Iowa

(i) The subprocessors engaged by WSP to provide the WSP Offerings.

1. *Microsoft Corporation*
2. *ACS Germany (if appropriate, as identified in the Order)*

Categories of personal data

In the event any SaaS Services are identified in the Order, depending on the version of the SaaS Services (Dialogue Cloud or Dialogue Cloud Neo), the following tables describe the categories of Personal Information that can be Processed by WSP to provide those SaaS Services:

1. Dialogue Cloud Neo (V3 and above)

Data	Containing	From/To	PII
Dialogue Cloud Service	• Agent Display Name • Agent UPN • Agent Object Id • Contact Center name • Address name • Address UPN • Address Object Id • Agent/Contact Center assignments • Address/Contact Center assignments • TenantId	Customer Azure AD /Neo configuration data/Communication events to Dialogue Cloud Neo SaaS database	EUII, OII OII
Data	Containing	From - To	PII
Dialogue Cloud Session Border Controllers syslogs	• Date/Time phone records • Customer company name • SIP and UPN addresses of agents • Phone numbers of customers and agents • IP addresses of customer SBC's	• Dialogue Cloud Session Border Controllers syslogs	• Dialogue Cloud Syslog server • No retention

Call Detail Records	• DateTime – Incoming Call • Customer Address (either phone number or object id) • Endpoint Address (either phone number or object id) • DateTime – Call Queued • Contact Center name in which the call is Queued • DateTime – Call Accepted • Agent Address (either phone number or object id) • DateTime – Call Transferred • Transferee Address (either phone number or object id) • DateTime – Call Disconnected	Raw events from Anywhere365 BackEnd to Event Store (cosmosDB) Read models for readable content, stored in CosmosDb/SQL (Optional) Readmodels pushes data to PowerBI Service of customer for live reporting	EUII, OII
DialogueCloud Backend Logfiles	• Request and response logging • Business logic logging; e.g. • DateTime – Incoming Call • Customer Address (either phone number or object id) • Endpoint Address (either phone number or object id) • DateTime – Call Queued • Contact Center name in which the call is Queued • DateTime – Call Accepted • Agent Address (either phone number or object id) • DateTime – Call Transferred • Transferee Address (either phone number or object id) • DateTime – Call Disconnected	Anywhere365 Dialogue Cloud Services to Dialogue Cloud Neo SaaS Azure Log Analytics workspace	EUII, OII

EUII: End User Identifiable Information. Data that identifies or could be used to identify the user of a Microsoft Service.
EUII: does not contain Customer content
OII: Organization Identifiable Information: Data that can be used to identify a tenant, generally config or usage data.

This data is not linkable to a user and does not contain Customer content.

***