# Exhibit 2 Data Processing Agreement for Dialogue Cloud

CUSTOMER (as defined below) and WSP (as defined below) have agreed to enter into this separate Data Processing Agreement (the “DPA”) pursuant to Section 11.1 of the DCA. The DPA forms an integral part of the Agreement (as defined below) as Exhibit 2.

## 1. BACKGROUND AND APPLICABILITY

1.1 CUSTOMER and WSP have entered into the Agreement (as defined below in Section 2) under which WSP shall provide certain products and/or services to the CUSTOMER. Within the scope and for the purpose of the performance of the Agreement, WSP will Process Personal Data on behalf of the CUSTOMER.

1.2 CUSTOMER and WSP have entered into this DPA in order to fulfill the requirement of a written agreement as set out in Applicable Data Protection Legislation. In addition to what may be set out in the Agreement, the following shall apply in relation to WSP’s Processing of Personal Data on behalf of the CUSTOMER.

## 2. INTERPRETATION AND DEFINITIONS

2.1 In this DPA, 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 "DPA" also refers to any amendment or supplement to it;
5. The term "including" means including without limitation;
6. Capitalized words, phrases and acronyms shall have the meanings given to them herein, elsewhere in the Agreement or shall have their ordinary (technical or other) meaning;
7. Parties have expressly required the DPA to be drawn up in English.

2.2 In the case of a conflict between any provision of this DPA and any other provisions set forth in the Agreement, the following descending order of precedence shall apply: (1) the provisions of the End Customer Agreement(s), (2) the provisions of this DPA, and (3) the provisions of the Order. In the event there is a conflict between the provisions of this DPA and the provisions of the Exhibits, the body of this DPA shall prevail, and only to the extent the provisions (of the body) meet the requirements as set forth in the then current Applicable Data Protection Legislation. By way of derogation from the previous sentences, Section 8 of this DPA shall always prevail.

2.3 "Agreement" means (as the context requires): (i) the End Customer Agreement and its Exhibits, or (ii) the agreement described under (i) and all Orders and other contract documents including this DPA (taken together) for the provisioning of certain products and/or services.

2.4 “Affiliate” means in relation to an entity, another entity controlling, controlled by, or under common control with that entity;

2.5 “Applicable Data Protection Legislation” means any national or internationally binding data protection laws or regulations applicable at any time during the term of this DPA to the Processing of Personal Data under the Agreement;

2.6 “Controller” means the legal entity which determines the purposes and means of the Processing of Personal Data as defined in the GDPR;

2.7 “CUSTOMER” means the party identified in the End Customer Agreement in effect between WSP or, if appropriate, its Partner on one hand and such party on the other hand.

2.8 “Data Protection Authorities” means any competent national data protection authority responsible for enforcing data privacy laws.

2.9 "Data Subject" means the natural person to whom the Personal Data is related as defined in the GDPR;

2.10 "EEA" means the European Economic Area;

2.11 "End Customer Agreement" means: (i) the Dialogue Cloud Agreement (DCA) (available via WSP's web site https://anywhere365.io/terms-conditions/) and, if parties to the DCA agree to enter into a separate Data Processing Agreement pursuant to Section 11.1 of the DCA, (ii) this DPA (available via WSP's web site https://anywhere365.io/terms-conditions/), entered into (directly or indirectly through a Partner) with the CUSTOMER, which specifies the rights and restrictions for the products and/or services, all as may be amended by WSP from time to time;

2.12 "Party" means the CUSTOMER or WSP;

2.13 "Processor" means the legal entity processing Personal Data on behalf of the Controller as defined in the GDPR;

2.14 "Personal Data" means any information relating to an identified or identifiable living, natural person as defined in the GDPR;

2.15 "Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed that likely represents a risk to CUSTOMER or CUSTOMER Personal Data;

2.16 "Processing" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction as defined in the GDPR;

2.17 "Subcontractor" means the legal entity which is engaged by WSP for carrying out Processing activities on behalf of WSP;

2.18 "WSP" means Workstreampeople B.V.

## 3. PROCESSING OF PERSONAL DATA

3.1 WSP undertakes to only Process Personal Data in accordance with documented instructions communicated from time to time by the CUSTOMER. CUSTOMER acknowledges that WSP is dependent on CUSTOMER's Microsoft Azure instance for the performance of its obligations under the Agreement including any Processing by WSP of CUSTOMER Personal Data. The CUSTOMER's initial instructions to WSP regarding the subject-matter of the Processing, the nature and purpose of the Processing, the type of Personal Data and categories of Data Subjects are set forth in this DPA and in Exhibit 1.

WSP shall assist the CUSTOMER, either as a Processor or as a Controller, in fulfilling its legal obligations under Applicable Data Protection Legislation. This may include but is not limited to the CUSTOMER's obligation to assist with and/or respond to requests for exercising the Data Subject's rights such as right of access, right to rectification, right to erasure, right to restriction of processing, right to data portability and right to object, as well as the CUSTOMER's obligation to ensure a level of security appropriate to the risk and to perform a data protection impact assessment. Secure erasure of data is based on the Azure policy of erasing data. This is part of the retention policy of Azure Log Analytics.

3.2 WSP shall immediately inform the CUSTOMER if WSP does not have sufficient instructions for how to Process Personal Data in a particular situation or if instructions provided under this DPA, in WSP's reasonable opinion, violates Applicable Data Protection Legislation.

3.3 If Data Subjects, Data Protection Authorities or any other competent third parties request information from WSP regarding the processing of Personal Data covered by this DPA, WSP shall refer such request to the CUSTOMER. WSP may not in any way act on behalf of or as a representative of the CUSTOMER and may not, without prior instructions from the CUSTOMER, transfer or in any other way disclose Personal Data or any other information relating to the Processing of Personal Data to any third party. In the event WSP, according to applicable laws and regulations, is required to disclose Personal Data that WSP Processes on behalf of the CUSTOMER, WSP shall, unless legally prevented, inform the CUSTOMER thereof immediately and shall request confidentiality in conjunction with the disclosure of requested information.

## 4. SUBCONTRACTORS

4.1 WSP will engage the Subcontractors set out in Exhibit 1 for the purposes specified therein. WSP undertakes to ensure that all Subcontractors are bound by written agreements that require them to comply with corresponding data processing obligations to those contained in this DPA.

4.2 In the event WSP wants to engage a Subcontractor other than those specified in Exhibit 1, WSP shall without undue delay and at the latest 8 weeks prior to transferring any Personal Data to such Subcontractor, inform the CUSTOMER, in writing, of the identity of such Subcontractor as well as the purpose for which it will be engaged, thereby giving the CUSTOMER the opportunity to object to such changes. The information shall also include information about the location of the Subcontractor and may not involve transfer of the Personal Data outside of the EEA unless approved by the CUSTOMER according to Section 5 below. WSP shall be fully liable to the CUSTOMER for the performance of the Subcontractor.

## 5. TRANSFER TO THIRD COUNTRIES

The location(s) of the Processing of Personal Data is/ are set out in Exhibit 1. WSP may not transfer Personal Data outside the EEA unless specifically approved in writing by the CUSTOMER and provided that adequate protection of the Personal Data in the receiving country is secured. In the event Parties agree to transfer Personal Data to third countries, the adequate protection in the receiving country shall be secured through an agreement incorporating the European Commission's Standard Contractual Clauses (processors), which will be included in Exhibit 2, between the Controller and the Processor (which receives the Personal Data in the country outside the EEA).

## 6. INFORMATION SECURITY AND CONFIDENTIALITY

6.1 Taking into account the state of the art and the costs of implementation and the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of the Data Subjects, WSP shall implement appropriate technical and organizational measures (please check Anywhere365 TOMs Document) to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(i) If appropriate, the pseudonymization and encryption of Personal Data;

(ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services Processing Personal Data;

(iii) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and

(iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing.

6.2 In assessing the appropriate level of security, WSP shall take into account the particular risks that are presented by Processing in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted stored or otherwise Processed.

6.3 WSP shall immediately and in any event not later than 24 hours after becoming aware of it notify the Personal Data Breach to the CUSTOMER. The notification shall at least:

(i) describe the nature of the Personal Data Breach including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;

(ii) communicate the name and contact details of the data protection officer or another contact point where more information can be obtained;

(iii) describe the likely consequences of the Personal Data Breach;

(iv) describe the measures taken or proposed to be taken by WSP to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects;

(v) include any other information available to WSP which the Controller is required by Applicable Data Protection Legislation to notify to the Data Protection Authorities and/or the Data Subjects.

WSP will furthermore provide the reasonable assistance requested by the CUSTOMER in order to investigate the Personal Data Breach and notify it to the Data Protection Authorities and/or the Data Subjects as required by Applicable Data Protection Legislation. This includes *inter alia* an obligation to document the Personal Data Breach (e.g. circumstances, impacts and remedial actions).

6.4 WSP undertakes to not disclose or otherwise make the Personal Data Processed under this DPA available to any third party, without the CUSTOMER's prior written approval. Notwithstanding the above, disclosure to a Subcontractor listed in Exhibit 1 or subsequently notified to the CUSTOMER in accordance with Section 4.2 above is permitted.

6.5 WSP undertakes to ensure that access to Personal Data under this DPA is restricted to those of its personnel who directly require access to the Personal Data in order to fulfill WSP's obligations in accordance with this DPA and the Agreement. WSP shall ensure that such personnel (whether employees or others engaged by WSP) is bound by a confidentiality obligation concerning the Personal Data to the same extent as WSP in accordance with this DPA.

6.6 The duties of confidentiality set forth in this Section 6 shall survive the expiry or termination of the DPA.

## 7. AUDIT RIGHTS

WSP undertakes to make available to the CUSTOMER all information and all assistance reasonably required by CUSTOMER to demonstrate compliance with the obligations laid down in this DPA. WSP will furthermore allow for and contribute to audits conducted by the CUSTOMER or a Data Protection Authority and in each case solely in relation to Processing of CUSTOMER Personal Data under this DPA.

## 8. LIABILITY AND INDEMNIFICATION

8.1 Notwithstanding the provisions in the Agreement, a Party shall be liable and indemnify, defend and hold harmless pursuant to clause 82 of the GDPR the other Party or its Affiliates for all damages (including damages resulting from loss of reputation or loss of data), fines, losses and costs, incurred and arising from or relating to non-compliance by the first Party (including its Subcontractors and Affiliates) with its obligations under the DPA or Applicable Data Protection Laws for Personal Data that it controls.

8.2 Notwithstanding the liability provisions in the Agreement, each Party shall indemnify the other Party against claims brought by third parties, including Data Subjects and Data Protection Authorities, and against all associated damage and reasonably incurred costs arising from non-compliance by the first Party (including its subcontractors and Affiliates) with obligations under the DPA.

8.3 Each Party's entire liability as referred to in Section 8.1 as well as the obligation to indemnify the other party in Section 8.2 is cumulatively limited to an amount equal to the limitations set forth in the Agreement.

8.4 Section 8.3 does not apply to liability or indemnification resulting from willful conduct or gross negligence or (if appropriate) to the extent any liability cannot be limited or excluded by law.

## 9. TERM

This DPA shall commence on the effective date of the DCA and run until as long as WSP Processes Personal Data on behalf of the CUSTOMER under the End Customer Agreement.

## 10. NOTICES

Any notice or other communication to be provided by one Party to the other Party under this DPA, shall be provided in accordance with the notices provision of the Agreement.

## 11. MEASURES UPON COMPLETION OF PROCESSING OF PERSONAL DATA

11.1 After the end of the delivery of the products and/or the provision of the products and/or services pursuant to the Agreement, WSP shall delete or return all Personal Data (including any copies thereof) to the CUSTOMER, as reasonably instructed by the CUSTOMER, and shall ensure that any Subcontractor does the same.

11.2 Upon request by the CUSTOMER, WSP shall provide a written notice of the measures taken with regard to the deletion or return of the Personal Data upon the completion of the Processing.

Version 202405

**Attachment 2.1 Data Processing Instructions**

| | | |
|---|---|---|
| **Purposes**<br>Specify all purposes for which the Personal Data will be processed by WSP | | WSP's performance of the (End Customer) Agreement. |
| **Data subjects**<br>Specify the categories of Data Subjects whose Personal Data will be Processed by WSP | | Company employees and, if appropriate, customers and business partners of CUSTOMER. |
| **Categories of Personal Data**<br>Specify the different types of Personal Data that will be Processed by WSP | | Please check table below |
| **Processing operations**<br>Specify all processing activities to be conducted by WSP | | As appropriate, processing CUSTOMER Personal Data for purposes of providing A365 Dialogue Cloud pursuant to the Agreement |
| **Subcontractor(s)**<br>Specify the Subcontractors engaged by WSP (if any) and the purposes for which the Personal Data is Processed by such Subcontractor | | 1. Microsoft Azure<br>2. If Deepdesk functionality is licensed to CUSTOMER, as specified in the Order: Deepdesk BV |
| **Location of processing operations**<br>Specify all locations where the Personal Data will be Processed by WSP* and any Subcontractor (if applicable) | | MS Azure DC controlled by WSP |
| * This excludes any CUSTOMER (Personal) Data that is stored in the Microsoft SQL Server in the Azure tenant and the SharePoint Online site collection as part of the Office365 tenant of the CUSTOMER (and which systems are not controlled by WSP). Customer is and remains the owner of the CUSTOMER (Personal) Data. | | |

**Table Categories of CUSTOMER Personal Data**

*Data classification: The log files mention are classified as Confidential (please also check Data Classification Policy)*

*Access: We implemented the Principle of Least Privilege, therefore cloud engineers will have access to this data if needed.*

| Data | Containing | From | To |
|---|---|---|---|
| **Dialogue Cloud conferencing backend log files** | ● Date/Time phone records<br>● Customer company name<br>● SIP and UPN addresses of agents<br>● Phone numbers of customers and agents<br>● IP addresses of end customers (only when WebChat is enabled) | ● Anywhere365 Dialogue Cloud conferencing backend | ● Azure Log Analytics Workspace (retention 30 days)<br>● Disk (retention 2 days) |
| **Dialogue Cloud Session Border Controllers syslogs** | ● Date/Time phone records<br>● Customer company name<br>● SIP and UPN addresses of agents<br>● Phone numbers of customers and agents<br>● IP addresses of customer SBC's | ● Dialogue Cloud Session Border Controllers syslogs | ● Dialogue Cloud Syslog server<br>● No retention |
| **SIP Traffic** | ● See RFC | ● Anywhere365 Dialogue Cloud conferencing backend | ● Dialogue Cloud Session Border Controllers<br>● Only stored on syslog server, see above<br>● Customer Sessions Border controllers |
| **Call Detail Records** | ● Date/Time phone records<br>● Customer company name<br>● and UPN addresses of agents<br>● Phone numbers of customers and agents<br>● IP addresses of end customers (only when WebChat is enabled) | ● Anywhere365 Dialogue Cloud conferencing backend<br>● Anywhere365 Dialogue Cloud Session Border Controllers | ● Azure SQL Database in customer tenant<br>● (optional) SharePoint Online Call Summary list in customer tenant<br>● Since data is stored in customer's tenant, they set retention policy |
| **Audio Recordings** | ● Actual audio recording of phone call | ● Anywhere365 Dialogue Cloud conferencing backend | ● SharePoint Online Library in customer tenant |

| | | | |
|---|---|---|---|
| | | | • If upload files, temporary stored on disk<br>• Since data is stored in customer’s tenant, they set retention policy |
| **Voice mail recordings** | • Actual audio recording of a voicemail message | • Anywhere365 Dialogue Cloud conferencing backend | • SharePoint Online Library in customer tenant<br>• If upload files, temporary stored on disk<br>• Since data is stored in customer’s tenant, they set retention policy |

**Attachment 2.2 Standard Contractual Clauses**

SCCs_EN_TXT.pdf **or** Publications Office (europa.eu)