# UK Public Sector Business and Services Agreement

This Microsoft Business and Services Agreement ("MBSA") is entered into by the entities identified on the signature form, and its terms and conditions are incorporated by reference into any Supplemental Agreement under which Customer or its Affiliates acquire Products or Professional Services.

## *1. Definitions.*

In this agreement, the following definitions apply:

"Affiliate" means any legal entity that controls, is controlled by, or that is under common control with a party. "Control" means ownership of more than a 50% interest of voting securities in an entity or the power to direct the management and policies of an entity.

"Customer" means *Crown Commercial Service, as* the entity that has entered into this agreement, *and other Government Entities.*

"Customer Data" means all data, including all text, sound, software, image or video files that are provided to Microsoft by, or on behalf of, Customer and its Affiliates through use of Online Services.

"day" means a calendar day.

"Fixes" means Product fixes, modifications or enhancements, or their derivatives, that Microsoft either releases generally (such as Product service packs), or provides to Customer to address a specific issue.

*"Government Entity" means Customer or a Public Sector entity that meets the eligibility criteria as defined in Annex 3 of the 2018 Digital Transformation Arrangements.*

*"License Agreement" means any license agreement expressly incorporating the terms of this MBSA.*

"Microsoft" means the Microsoft Affiliate that has entered into this agreement and its Affiliates, as appropriate.

"Online Services" means the Microsoft-hosted services identified as Online Services in the Product Terms.

"Online Services Terms" means the additional terms that apply to Customer's use of Online Services published on the Volume Licensing Site and updated from time to time.

"Pre-Existing Work" means any computer code or other written materials developed or otherwise obtained independent of this agreement.

"Product" means all products identified in the Product Terms, such as all Software, Online Services and other web-based services, including pre-release or beta versions. Product availability may vary by region.

"Product Terms" means the document that provides information about Microsoft Products and Professional Services available through volume licensing. The Product Terms document is published on the Volume Licensing Site and is updated from time to time.

"Professional Services" means Product support services and Microsoft consulting services provided to Customer under this agreement. "Professional Services" does not include Online Services.

"SLA" means Service Level Agreement, which specifies the minimum service level for Online Services and is published on the Volume Licensing Site.

"Services Deliverables" means any computer code or materials, other than Products or Fixes, that Microsoft leaves with Customer at the conclusion of Microsoft's performance of Professional Services.

"Software" means licensed copies of Microsoft software identified on the Product Terms. Software does not include Online Services or Services Deliverables, but Software may be part of an Online Service.

"Statement of Services" means any work orders or other description of Professional Services that incorporates this MBSA.

"Supplemental Agreement" means any agreement that incorporates this MBSA.

"Trade Secret" means information that is not generally known or readily ascertainable to the public, has economic value as a result, and has been subject to reasonable steps under the circumstances to maintain its secrecy.

"use" or "run" means to copy, install, use, access, display, run or otherwise interact with.

"Use Rights" means the use rights or terms of service for each Product published on the Volume Licensing Site and updated from time to time. The Use Rights supersede the terms of any end user license agreement that accompanies a Product. The Use Rights for Software are published by Microsoft in the Product Terms. The Use Rights for Online Services are published in the Online Services Terms.

"Volume Licensing Site" means http://www.microsoft.com/licensing/contracts or a successor site.

## 2. *Use, ownership, rights, and restrictions.*

**a. Products.** Unless otherwise specified in a Supplemental Agreement, use of any Product is governed by the Use Rights specific to each Product and version and by the terms of the applicable Supplemental Agreement.

**b. Fixes and Services Deliverables.**

**(i) Fixes.** Each Fix is licensed under the same terms as the Product to which it applies. If a Fix is not provided for a specific Product, any use rights Microsoft provides with the Fix will apply.

**(ii) Pre-Existing Work.** All rights in Pre-existing Work will remain the sole property of the party providing it. Each party may use, reproduce and modify the other party's Pre-existing Work only as needed to perform obligations related to Professional Services.

**(iii) Services Deliverables.** Upon payment in full for the Professional Services, Microsoft grants Customer a non-exclusive, non-transferable, perpetual license to reproduce, use and modify the Services Deliverables solely for Customer's internal business purposes, subject to the terms and conditions in this agreement.

**(iv) Affiliates' rights.** Customer may sublicense its rights in Services Deliverables to its Affiliates, but Customer's Affiliates may not sublicense these rights. Customer is liable for ensuring its Affiliates' compliance with this agreement.

**c. Non-Microsoft software and technology.** Customer is solely responsible for any non-Microsoft software or technology that it installs or uses with the Products, Fixes, or Services Deliverables.

**d. Restrictions.** Customer must not (and is not licensed to) (1) reverse engineer, decompile or disassemble any Product, Fix, or Services Deliverable; (2) install or use non-Microsoft software or technology in any way that would subject Microsoft's intellectual property or technology to any other license terms; or (3) work around any technical limitations in a Product, Fix or Services Deliverable or restrictions in Product documentation. Except as expressly permitted in this agreement, a Supplemental Agreement or Product documentation, Customer must not (and is not licensed to) (1) separate and run parts of a Product or Fix on more than one device, upgrade or downgrade parts of a Product or Fix at different times, or transfer parts of a Product or Fix separately; or (2) distribute, sublicense, rent, lease, lend any Products, Fixes, or Services Deliverables, in whole or in part, or use them to offer hosting services to a third party.

**e. Reservation of rights.** Products, Fixes, and Services Deliverables are protected by copyright and other intellectual property rights laws and international treaties. Microsoft reserves all rights not expressly granted in this agreement. No rights will be granted or implied by waiver or estoppel. Rights to access or use Software on a device do not give Customer any right to implement Microsoft patents or other Microsoft intellectual property in the device itself or in any other software or devices.

## 3. *Confidentiality.*

**a.** "Confidential Information" is non-public information that is designated "confidential" or that a reasonable person should understand is confidential, including Customer Data and the terms of Microsoft agreements. The Online Services Terms may provide additional obligations for,

and limitations on disclosure and use of, Customer Data. Confidential Information does not include information that (1) becomes publicly available without a breach of this agreement, (2) the receiving party received lawfully from another source without a confidentiality obligation, (3) is independently developed, or (4) is a comment or suggestion volunteered about the other party's business, products or services.

**b.** Each party will take reasonable steps to protect the other's Confidential Information and will use the other party's Confidential Information only for purposes of the parties' business relationship. Neither party will disclose that Confidential Information to third parties, except to its employees, Affiliates, contractors, advisors and consultants ("Representatives") and then only on a need-to-know basis under nondisclosure obligations at least as protective as this agreement. Each party remains responsible for the use of the Confidential Information by its Representatives and, in the event of discovery of any unauthorized use or disclosure, must promptly notify the other party.

**c.** A party may disclose the other's Confidential Information if required by law; but only after it notifies the other party (if legally permissible) to enable the other party to seek a protective order.

**d.** Neither party is required to restrict work assignments of its Representatives who have had access to Confidential Information. Each party agrees that the use of information retained in Representatives' unaided memories in the development or deployment of the parties' respective products or services does not create liability under this agreement or trade secret law, and each party agrees to limit what it discloses to the other accordingly.

**e.** These obligations apply (1) for Customer Data until it is deleted from the Online Services, and (2) for all other Confidential Information, for a period of five years after a party receives the Confidential Information.

***f. Use of Confidential Information relating to License Agreement pricing***

**(i)** *Government Entities and Microsoft may disclose any specific negotiated or amended terms and the pricing terms set out in a License Agreement together with details of the desktop or user numbers and products licensed under a License Agreement to Crown Commercial Service and any other Government Entities.*

**(ii)** *Either party may disclose the pricing terms relating to a License Agreement to resellers or software advisors appointed by Government Entities.*

**(iii)** *Disclosures of pricing information shall be conspicuously marked "Restricted Commercial" (or marked in a similar and prominent fashion).*

***g. Disclosing confidential information pursuant to a request under the Freedom of Information Act.*** *Microsoft acknowledges that Government Entities may be subject to the provisions of the Freedom of Information Act 2000 or the Freedom of Information (Scotland) Act 2002 ("the FOIA Acts") and that under the FOIA Acts may be required to disclose Microsoft Confidential Information. If a Government Entity receives a request to disclose Confidential Information under the FOIA Acts, it shall notify and consult with Microsoft as soon as is reasonably practicable after receipt of the request and shall seek Microsoft's view on whether such Confidential Information may fall under one of the exemptions to disclosure under the FOIA Acts. Taking into account Microsoft's view on whether an exemption should apply, the Customer shall be responsible for determining whether any Confidential Information and/or any other information is exempt from disclosure in accordance with the FOIA Acts. Microsoft shall use reasonable endeavours to provide Government Entities with such assistance as is reasonably necessary to respond to a request under the FOIA Acts within the timeframes specified in the FOIA Acts. Microsoft shall not respond directly to any request under the FOIA Acts without the approval of the applicable Governement Entity.*

## *4. Privacy and compliance with laws.*

**a.** Customer consents to the processing of personal information by Microsoft and its agents to facilitate the subject matter of this agreement. Customer will obtain all required consents from third parties (including Customer's contacts, resellers, distributors, administrators, and employees) under applicable privacy and data protection law before providing personal information to Microsoft.

b. Personal information collected under this agreement (1) may be transferred, stored and processed in the United States or any other country in which Microsoft or its service providers maintain facilities and (2) will be subject to the privacy terms specified in the Use Rights. Microsoft will abide by the requirements of European Economic Area and Swiss data protection law regarding the collection, use, transfer, retention, and other processing of personal data from the European Economic Area and Switzerland.

c. **U.S. export.** Products, Fixes, and Services Deliverables are subject to U.S. export jurisdiction. Customer must comply with all applicable international and national laws, including the U.S. Export Administration Regulations, the International Traffic in Arms Regulations, and end-user, end use and destination restrictions by U.S. and other governments related to Microsoft products, services, and technologies.

## *5. Warranties.*

a. **Limited warranties and remedies**.

(i) **Software.** Microsoft warrants that each version of the Software will perform substantially as described in the applicable Product documentation for one year from the date Customer is first licensed for that version. If it does not, and Customer notifies Microsoft within the warranty term, then Microsoft will, at its option (1) return the price Customer paid for the Software license, or (2) repair or replace the Software.

(ii) **Online Services.** Microsoft warrants that each Online Service will perform in accordance with the applicable SLA during Customer's use. Customer's remedies for breach of this warranty are in the SLA.

(iii) **Professional Services.** Microsoft warrants that it will perform Professional Services with professional care and skill. If Microsoft fails to do so, and Customer notifies Microsoft within 90 days of the date the Professional Services were performed, then Microsoft will, at its discretion, either re-perform the Professional Services or return the price Customer paid for them.

The remedies above are Customer's sole remedies for breach of the warranties in this section. Customer waives any breach of warranty claims not made during the warranty period.

b. **Exclusions.** The warranties in this agreement do not apply to problems caused by accident, abuse or use in a manner inconsistent with this agreement, including failure to meet minimum system requirements. These warranties do not apply to free, trial, pre-release, or beta products, or to components of Products that Customer is permitted to redistribute.

c. **Disclaimer. Except for the limited warranties above, Microsoft provides no other warranties or conditions and disclaims any other express, implied or statutory warranties, including warranties of quality, title, non-infringement, merchantability, and fitness for a particular purpose.**

## *6. Defense of third party claims.*

The parties will defend each other against the third-party claims described in this section and will pay the amount of any resulting adverse final judgment or approved settlement, but only if the defending party is promptly notified in writing of the claim and has the right to control the defense and any settlement of it. The party being defended must provide the defending party with all requested assistance, information, and authority. The defending party will reimburse the other party for reasonable out-of-pocket expenses it incurs in providing assistance. This section describes the parties' sole remedies and entire liability for such claims.

a. **By Microsoft.** Microsoft will defend Customer against any third-party claim to the extent it alleges that a Product, Fix or Services Deliverable made available by Microsoft for a fee and used within the scope of the license granted (unmodified from the form provided by Microsoft and not combined with anything else) misappropriates a trade secret or directly infringes a patent, copyright, trademark or other proprietary right of a third party. If Microsoft is unable to resolve a claim of infringement under commercially reasonable terms, it may,

at its option, either (1) modify or replace the Product, Fix or Services Deliverable with a functional equivalent; or (2) terminate Customer's license and refund any prepaid license fees (less depreciation on a five-year, straight-line basis) for perpetual licenses and any amount paid for Online Services for any usage period after the termination date. Microsoft will not be liable for any claims or damages due to Customer's continued use of a Product, Fix, or Services Deliverable after being notified to stop due to a third-party claim.

b. **By Customer.** To the extent permitted by applicable law, Customer will defend Microsoft against any third-party claim to the extent it alleges that: (1) any Customer Data or non-Microsoft software hosted in an Online Service by Microsoft on Customer's behalf misappropriates a trade secret or directly infringes a patent, copyright, trademark, or other proprietary right of a third party; or (2) Customer's use of any Product, Fix, or Services Deliverable alone or in combination with anything else, violates the law or damages a third party.

## *7. Limitation of liability.*

For each Product or Professional Service, each party's maximum, aggregate liability to the other under each Supplemental Agreement is limited to direct damages finally awarded in an amount not to exceed the amounts Customer was required to pay for the applicable Products or Professional Services during the term of the Supplemental Agreement, subject to the following:

a. **Online Services**. For Online Services, Microsoft's maximum liability to Customer for any incident giving rise to a claim will not exceed the amount Customer paid for the Online Service during the 12 months before the incident.

b. **Free Products and Distributable Code.** For Products and Professional Services provided free of charge and code that Customer is authorized to redistribute to third parties without separate payment to Microsoft, Microsoft's liability is limited to direct damages finally awarded up to US$5,000.

c. **Exclusions.** In no event will either party be liable for indirect, incidental, special, punitive, or consequential damages, or for loss of use, loss of business information, loss of revenue, or interruption of business, however caused or on any theory of liability.

d. **Exceptions.** No limitation or exclusions will apply to liability arising out of either party's (1) confidentiality obligations (except for all liability related to Customer Data, which will remain subject to the limitations and exclusions above); (2) defense obligations; or (3) violation of the other party's intellectual property rights.

## *8. Verifying compliance.*

a. **Right to verify compliance.** Customer must keep records relating to all use and distribution of Products by Customer and its Affiliates. Microsoft has the right, at its expense, to verify compliance with the Products' license terms. *To verify compliance, Microsoft will engage an independent auditor from an internationally recognised public accounting firm which will be subject to a condfidentially obligation at least equivalent to those obligations which are binding upon the Customer and Microsoft.* Customer must promptly provide the independent auditor with any information the auditor reasonably requests in furtherance of the verification, including access to systems running the Products and evidence of licenses for Products Customer hosts, sublicenses, or distributes to third parties. Customer agrees to complete Microsoft's self-audit process, which Microsoft may require as an alternative to a third party audit. *Any information collected in a self-audit will be used solely for purposes of determining compliance.*

b. **Remedies for non-compliance.** If verification or self-audit reveals any unlicensed use of Products, then within 30 days (1) Customer must order sufficient licenses to cover its use, and (2) if unlicensed use or distribution is 5% or more, Customer must reimburse Microsoft for the costs Microsoft incurred in verification and acquire the necessary additional licenses at 125% of the price, based on the then-current price list and Customer price level. The unlicensed use percentage is based on the total number of licenses purchased for current use compared to actual install base. If there is no unlicensed use, Microsoft will not subject Customer to another verification for at least one year. By exercising the rights and

procedures described above, Microsoft does not waive its rights to enforce this agreement or to protect its intellectual property by any other legal means.

c. **Verification process.** Microsoft will notify Customer at least 30 days in advance of its intent to verify Customer's compliance with the license terms for the Products Customer and its Affiliates use or distribute. *This verification will only take place if Microsoft has reasonable grounds for considering such verification being necessary.* This verification will take place during normal business hours and in a manner that does not interfere unreasonably with Customer's operations. *Prior to any verification, discussion with Crown Commercial Service will take place. Customer will be offered the option to undertake a Software Asset Management Review ("SAM Review") which Customer must complete within 12 months from the date of such offer. Only if Customer fails to complete such SAM Review within this timeframe, will Microsoft start the verification process.*

## 9. *Term and termination.*

a. **Term.** The effective date of this MBSA will be the earlier of either the date the MBSA is executed by Microsoft or the effective date of the first Supplemental Agreement. The MBSA is effective until terminated by a party, as described below.

b. **Termination.** Either party may terminate this MBSA on 60 days' notice. Termination will not affect any existing orders or Supplemental Agreements, but Customer will no longer be able to enter into Supplemental Agreements after the effective date of termination.

c. **Professional Services termination.** If Customer terminates a Statement of Services as a result of a breach by Microsoft, Customer must pay all amounts due under the Statement of Services as of the termination date. Upon Microsoft's receipt of payment for the Professional Services, Customer's interests in the Services Deliverables will vest. Microsoft has no obligation to continue to provide Professional Services if Customer fails to make timely payment for the Professional Services.

## 10. *Miscellaneous.*

a. **Use of contractors.** Microsoft may use contractors to perform services, but will be responsible for their performance, subject to the terms of this agreement.

b. **Microsoft as independent contractor.** The parties are independent contractors. Customer and Microsoft each may develop products independently without using the other's Confidential Information.

c. **Notices.** Notices to Microsoft must be sent to the address on the signature form. Notices must be in writing and will be treated as delivered on the date shown on the return receipt or on the courier or fax confirmation of delivery. Microsoft may provide information to Customer about upcoming ordering deadlines, services and subscription information in electronic form, including by email to contacts provided by Customer. Emails will be treated as delivered on the transmission date.

d. **Agreement not exclusive.** Customer is free to enter into agreements to license, use, or promote non-Microsoft products or services.

e. **Amendments.** Any amendment to this agreement must be executed by both parties, except that Microsoft may change the Product Terms and Use Rights from time to time, subject to the terms of this agreement. Any additional or conflicting terms and conditions contained in Customer's or a Partner's purchase order are expressly rejected and will not apply. Microsoft may require Customer to sign a new agreement or an amendment to an existing agreement before processing a new order or entering into a Supplemental Agreement.

f. **Assignment.** Either party may assign this agreement to an Affiliate, but it must notify the other party in writing of the assignment. Any other proposed assignment must be approved by the non-assigning party in writing. Assignment will not relieve the assigning party of its obligations under the assigned agreement. Any attempted assignment without required approval will be void.

g. **Applicable law.** *The terms of this MBSA and any Supplemental Agreement entered into under this MBSA will be governed by and construed in accordance with the laws of England and Wales.* The 1980 United Nations Convention on Contracts for the International Sale of Goods and its related instruments will not apply to this agreement.

h. **Dispute resolution.** *When bringing an action to enforce this MBSA or any issues arising from it, (including any Supplemental Agreement), the parties agree to the jurisdiction of the English courts. The parties shall first attempt to resolve disputes informally and in good faith. If the dispute cannot be resolved within 30 days of the dispute arising (or such period as may be agreed by the parties), the parties shall refer all matters in dispute for consideration and decision by designated senior managers, who shall use their reasonable endeavours to reach a solution to any such dispute within a period of 14 days following receipt of notice of such dispute arising (or such other period as may be agreed by the parties). If the dispute cannot be resolved by the parties' representatives as set out above, the dispute may be referred to mediation by the agreement of the parties. In the event that mediation does not succeed in finding a resolution to the dispute within a period of 30 days, or such other time as the parties may agree, the parties may agree to arbitration or either party may take such action as is available to it under this Agreement or generally at law. Nothing in this section 10.h. shall be construed to preclude any party from seeking injunctive relief in order to protect its rights during escalation and mediation.*

i. **Severability.** If any provision in this agreement is held to be unenforceable, the balance of the agreement will remain in full force and effect.

j. **Waiver.** Failure to enforce any provision of this agreement will not constitute a waiver. Any waiver must be in writing and signed by the waiving party.

k. **No third-party beneficiaries.** This Agreement does not create any third-party beneficiary rights.

l. **Survival.** All provisions survive termination or expiration of this agreement except those requiring performance only during the term of the agreement.

m. **Professional Services payment terms.** Customer agrees to pay all fees in a Statement of Services within 30 days of the date of invoice, unless the Statement of Services provides otherwise. Microsoft may assess a finance charge of the lesser of 18% per annum, accrued, calculated and payable monthly, or the highest amount allowed by law, on all past due amounts due to Microsoft. Microsoft will have no obligation to continue to provide Professional Services if Customer fails to make timely payment.

n. **Taxes.** If any amounts are to be paid to Microsoft, the amounts owed are exclusive of any taxes unless otherwise specified on the invoice as tax inclusive. Customer shall pay all value added, goods and services, sales, gross receipts, or other transaction taxes, fees, charges, or surcharges, or any regulatory cost recovery surcharges or similar amounts that are owed under this agreement and that Microsoft is permitted to collect from Customer under applicable law. Customer shall be responsible for any applicable stamp taxes and for all other taxes that it is legally obligated to pay, including any taxes that arise on the distribution or provision of Products or Professional Services by Customer to its Affiliates. Microsoft shall be responsible for payment of all taxes based upon its net income, gross receipts taxes imposed in lieu of taxes on income or profits, or taxes on Microsoft's property ownership.

   If any taxes are required to be withheld on payments made to Microsoft, Customer may deduct such taxes from the amount owed and pay them to the appropriate taxing authority; provided, however, that Customer promptly secures and delivers to Microsoft an official receipt for those withholdings and other documents Microsoft reasonably requests to claim a foreign tax credit or refund. Customer must ensure that any taxes withheld are minimized to the extent possible under applicable law.

o. ***Insurance.*** *Microsoft will procure and maintain the following insurance coverage at all times when performing Professional Services on Customer's premises under this agreement via commercial insurance, self-insurance, a combination of the two or any other similar risk financing alternative:*

   **(i)** *Commercial General Liability covering bodily injury and tangible property damage liability with a limit of not less than U.S. $2,000,000 each occurrence;*

(ii) *Workers' Compensation (or maintenance of a legally permitted and governmentally-approved program of self-insurance) covering Microsoft employees pursuant to applicable state workers' compensation laws for work-related injuries suffered by Microsoft's employees;*

(iii) *Employer's Liability with limits of not less than U.S. $1,000,000 per accident;*

(iv) *Professional Liability/Errors & Omissions Liability covering damages arising out of negligent acts, errors, or omissions committed by Microsoft or its employees in the performance of Services, with a limit of liability of not less than U.S. $2,000,000 per claim; and*

(v) *Automobile Liability (if vehicles are brought on Customer's premises or used in the performance of the Services) with U.S. $2,000,000 combined limit per occurrence, for bodily injury and property damage combined covering owned, non-owned and hired vehicles.*

Microsoft will provide Customer with evidence of coverage on request.

# Microsoft Professional Services Data Protection Addendum

November 1, 2017

Microsoft

# Introduction

This Microsoft Professional Services Data Protection Addendum ("Addendum") applies solely to the Microsoft Professional Services (defined below) provided under the Agreement. This Addendum covers Support and Consulting Data provided in connection with Consulting Services or when submitted to receive technical support for Premier through the Microsoft Support Portal, Premier Phone Support, or other approved submission mechanisms as described in the Microsoft Trust Center under Commercial Support. This Addendum does not apply to other Microsoft Professional Services offers including Microsoft Managed Services for the Cloud, Office 365 FastTrack, and technical support provided outside of Premier Support such as support requests submitted through the Microsoft Online Services Administrative Portals as well as Premier support requests escalated to Microsoft Products or Online Services engineering or operations for resolution.

This Addendum does not supersede any other Data Protection Agreement signed by the parties unless otherwise agreed in writing; however, in the absence of other agreed upon GDPR terms, the terms of Attachment 3 – European Union General Data Protection Regulation Terms will apply.

# General Terms

### Definitions

Capitalized terms used but not defined in this Addendum will have the meanings provided in the Agreement. The following defined terms are used in this Addendum:

"Agreement" means the Description of Services and any Exhibits, Statements of Work, Enterprise Services Work Order(s), and the Microsoft Master Agreement identified above.

"Consulting Services" means professional planning, advice, guidance, data migration, deployment and solution/software development services provided by Microsoft under an Enterprise Services Work Order.

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

"Personal Data" means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"Professional Services" means Support Services and Consulting Services. The Professional Services do not include Microsoft's Online Services. Standard Contractual Clauses means the agreement attached to this Addendum as Attachment 1 and Attachment 2 pursuant to European Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under the EU Data Protection Directive.

"Support and Consulting Data" means all data, including all text, sound, video, image files, or software, that are provided to Microsoft by, or on behalf of, Customer (or that Customer authorizes Microsoft to obtain from an Online Service) through an engagement with Microsoft to obtain Professional Services covered under this Addendum.

"Support Services" means Support Services as described in the Description of Services or the Support and Consulting Description of Services, which consist of professional technical software support services provided by Microsoft that help customers identify and resolve issues in their information technology environment.

### Compliance with Laws

Microsoft complies with all data protection and privacy laws generally applicable to Microsoft's provision of the Professional Services. However, Microsoft is not responsible for compliance with any data protection or privacy laws or regulations applicable to Customer or Customer's industry that are not generally applicable to information technology service providers.

# Privacy

### Use of Support and Consulting Data

Microsoft will process Support and Consulting Data in accordance with the provisions of this Addendum and, except as stated in the Agreement and this Addendum, Microsoft (1) will acquire no rights in Support and Consulting Data and (2) will not use or disclose Support and Consulting Data for any purpose other than stated below. Microsoft's use of Support and Consulting Data is as follows:

- Support and Consulting Data will be used only to provide Customer the Professional Services. Microsoft will not use Support and Consulting Data or derive information from it for any advertising or similar commercial purposes.

### Processing of Personal Data

Article 28(1) of the GDPR requires an agreement between a controller and processor, and between a processor and subprocessor, that processing be conducted in accordance with technical and organizational measures that meet the requirements of the GDPR and ensure the protection of the rights of data subjects. The GDPR Terms in Attachment 3 are intended to satisfy that requirement for the parties. The GDPR Terms are organized as follows:

- Section C reproduces (with minor edits for clarity) the relevant contractual terms required of processors and controllers by Articles 28, 32, and 33 of the GDPR.
- Appendix 1 provides more details on what Customer can expect from Microsoft to fulfill those terms, as well as Microsoft's commitments with regard to Articles 30 and 34-36 of the GDPR.

Microsoft makes the commitments in the GDPR Terms to all customers effective May 25, 2018.

### Disclosure of Support and Consulting Data

Microsoft will not disclose Support and Consulting Data outside of Microsoft or its controlled subsidiaries and affiliates except (1) as Customer directs, (2) as described in this Addendum, or (3) as required by law.

Microsoft will not disclose Support and Consulting Data to law enforcement unless required by law. If law enforcement contact Microsoft with a demand for Support and Consulting Data, Microsoft will attempt to redirect the law enforcement agency to request that data directly from Customer. If compelled to disclose Support and Consulting Data to law enforcement, Microsoft will promptly notify Customer and provide a copy of the demand unless legally prohibited from doing so.

Upon receipt of any other third party request for Support and Consulting Data, Microsoft will promptly notify Customer unless prohibited by law. Microsoft will reject the request unless required by law to comply. If the request is valid, Microsoft will attempt to redirect the third party to request the data directly from Customer.

In support of the above, Microsoft may provide Customer's basic contact information to the third party.

### Support and Consulting Data Deletion and Return

Microsoft will delete or return all copies of Support and Consulting Data after the business purposes for which the Support and Consulting Data was collected or transferred have been fulfilled, or earlier upon Customer's written request.

### End user Requests

Microsoft will not independently respond to requests from Customer's employees, agents or customers without Customer's prior written consent, except where required by applicable law.

### Location of Data Processing

Support and Consulting Data that Microsoft processes on Customer's behalf may be transferred to, and stored and processed in, the United States or any other country in which Microsoft or its Affiliates or subcontractors maintain facilities. Customer appoints Microsoft to perform any such transfer of Support and Consulting Data to any such country and to store and process Support and Consulting Data in order to provide the Professional Services.

Microsoft will abide by the requirements of European Economic Area and Swiss data protection law regarding the collection, use, transfer, retention, and other processing of Personal Data from the European Economic Area and Switzerland. Upon the start of enforcement of the GDPR, Microsoft will ensure that transfers of Personal Data to a third country or an international organization are subject to appropriate safeguards as described in Article 46 of the GDPR and that such transfers and safeguards are documented according to Article 30(2) of the GDPR. In addition to Microsoft's commitments under the Standard Contractual Clauses and other model contracts, Microsoft is certified to the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks and the commitments they entail. Microsoft agrees to notify Customer in the event that it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Privacy Shield principles.

All Support Services, and upon confirmation Consulting Services, also include the "Standard Contractual Clauses," pursuant to the European Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under the EU Data Protection Directive. The Standard Contractual Clauses are in Attachment 1 and Attachment 2.

The Standard Contractual Clauses are applicable for Consulting Services upon confirmation from ServicesEUMC@microsoft.com. The process for obtaining such confirmation can be initiated at http://aka.ms/ServicesEUMC.
In addition,

- Execution of the Agreement includes execution of Attachment 1 and Attachment 2, which is countersigned by Microsoft Corporation and Microsoft Global Services Center (India) Private Limited;

- The terms in Customer's Agreement, including this Addendum, constitute a data processing agreement under which Microsoft is the data processor; and
- Customer may opt out of the "Standard Contractual Clauses" or this Addendum (excluding GDPR Terms). To opt out, Customer must send the following information to Microsoft in a written notice (under terms of the Customer's Agreement):
    - the full legal name of the Customer and any Affiliate that is opting out;
    - if opting out of this Addendum (excluding GDPR Terms), a statement that Customer (or Affiliate) opts out of this Addendum (excluding GDPR Terms); and
    - if opting out of only the Standard Contractual Clauses, a statement that Customer (or Affiliate) opts out of the Standard Contractual Clauses only.
- In countries where regulatory approval is required for use of the Standard Contractual Clauses, the Standard Contractual Clauses cannot be relied upon under European Commission 2010/87/EU (of February 2010) to legitimize export of data from the country, unless Customer has the required regulatory approval.

**Microsoft Personnel**
Microsoft personnel will not process Support and Consulting Data without authorization from Customer. Microsoft personnel are obligated to maintain the security and secrecy of any Support and Consulting Data and this obligation continues even after their engagement ends. Microsoft shall provide periodic and mandatory data privacy and security training and awareness to its employees with access to Support and Consulting Data in accordance with laws applicable to Microsoft as a provider of professional IT services, and industry standards.

**Use of Subcontractors**
Microsoft may hire subcontractors to provide Professional Services on its behalf. Any such subcontractors will be permitted to obtain Support and Consulting Data only to deliver the services Microsoft has retained them to provide and will be prohibited from using Support and Consulting Data for any other purpose. Microsoft remains responsible for its subcontractors' compliance with the obligations of this Addendum. Any subcontractors to whom Microsoft transfers Support and Consulting Data, even those used for storage purposes, will have entered into written agreements with Microsoft or one of its Affiliates requiring that are not less protective than this Addendum. Customer consents to Microsoft's transfer of Support and Consulting Data to subcontractors as described in this Addendum.

For Customers with Standard Contractual Clauses, Microsoft provides a website that lists subcontractors authorized to access Support and Consulting Data for Support Services. At least 14 days before authorizing any new subcontractor to access Support and Consulting Data, Microsoft will update the website and provide Customer with a mechanism to obtain notice of that update. If Customer does not approve of a new subcontractor, then Customer may terminate the affected Professional Services by providing, before the end of the notice period, written notice of termination in accordance with the termination provisions of the applicable Master Agreement that includes an explanation of the grounds for non-approval.

Microsoft will not transfer to any third party (not even for storage purposes) personal data Customer provides to Microsoft in connection with the Professional Services.

# Customer Responsibilities

Customer must comply with applicable laws and regulations related to privacy, data protection, and confidentiality of communications related to its procurement and use of the Professional Services and its transfer of Support and Consulting Data to Microsoft.

Customer is responsible for obtaining necessary consents from individuals and for notifying individuals of transfer of their personal data from Customer to Microsoft.

# Additional European terms

If the Support and Consulting Data necessarily includes personal data about individuals in the European Economic Area or Switzerland, the additional terms in this Section 4 will apply. Terms used in this Section that are not specifically defined will have the meaning in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("EU Data Protection Directive").

**Intent of the Parties**

For all Professional Services, Customer is the data controller and Microsoft is a data processor (or sub-processor) acting on Customer's behalf. As data processor (or sub-processor), Microsoft will only act upon Customer's instructions. This Addendum and the Agreement (including the terms

and conditions incorporated by reference therein) are Customer's complete and final instructions to Microsoft for the processing of Support and Consulting Data. Any additional or alternate instructions may only be issued by Customer's business contact for the Professional Services and must be agreed to according to the process for amending the Agreement.

### Duration and Object of Data Processing

The duration of data processing shall be for the term designated under the Agreement. The objective of the data processing is the performance of the Professional Services.

### Scope and Purpose of Data Processing

The scope and purpose of processing of Support and Consulting Data, including any personal data included in the Support and Consulting Data, is described in this Addendum and the Agreement.

### Support and Consulting Data Access

For the term designated under the Agreement Microsoft will, at its election and as necessary under applicable law implementing Article 12(b) of the EU Data Protection Directive, either: (1) provide Customer with the ability to correct, delete, or block Support and Consulting Data, or (2) make such corrections, deletions, or blockages on Customer's behalf.

### Privacy Officer

Microsoft's privacy representative for the European Economic Area and Switzerland can be reached at the following address:

Microsoft Ireland Operations Ltd.

Attn: Data Protection

One Microsoft Place

South County Business Park

Leopardstown

Dublin 18, D18 P521, Ireland

# Security

### General Practices

Microsoft is committed to helping protect the security of Customer's information. Microsoft has implemented and will maintain and follow appropriate technical and organizational measures intended to protect Support and Consulting Data against accidental, unauthorized or unlawful access, disclosure alteration, loss or destruction and against all other unlawful forms of processing as stipulated in Exhibit 1 (the "TOMs"). Microsoft may update and/or amend the TOMs from time to time, but will not diminish the level of data protection provided. Upon Customer's written request, Microsoft will issue a statement re-confirming its compliance with the TOMs. The security measures described in Exhibit 1 are Microsoft's only responsibility with respect to the security of Support and Consulting Data.

### Exhibit 1 – Technical and Organizational Measure

| Domain | Practices |
|---|---|
| Organization of Information Security | **Security Ownership.** Microsoft has appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures.<br>**Security Roles and Responsibilities.** Microsoft personnel with access to Support and Consulting Data are subject to confidentiality obligations.<br>**Risk Management Program.** Microsoft performed a risk assessment before processing the Support and Consulting Data. Microsoft retains its security documents pursuant to its retention requirements after they are no longer in effect. |
| Asset Management | **Asset Inventory.** Microsoft maintains an inventory of all media on which Support and Consulting Data is stored. Access to the inventories of such media is restricted to Microsoft personnel authorized in writing to have such access.<br>**Asset Handling.**<br>- Microsoft classifies Support and Consulting Data to help identify it and to allow for access to it to be appropriately restricted (e.g., through encryption).<br>- Microsoft imposes restrictions on printing Support and Consulting Data and has procedures for disposing of printed materials that contain Support and Consulting Data. |

| Domain | Practices |
|---|---|
| | - Microsoft personnel must obtain Microsoft authorization prior to storing Support and Consulting Data on portable devices, remotely accessing Support and Consulting Data, or processing Support and Consulting Data outside Microsoft's facilities. |
| Human Resources Security | **Security Training**. Microsoft informs its personnel about relevant security procedures and their respective roles. Microsoft also informs its personnel of possible consequences of breaching the security rules and procedures. Microsoft will only use anonymous data in training. |
| Physical and Environmental Security | **Physical Access to Facilities.** Microsoft limits access to facilities where information systems that process Support and Consulting Data are located to identified authorized individuals.<br>**Physical Access to Components.** Microsoft maintains records of the incoming and outgoing media containing Support and Consulting Data, including the kind of media, the authorized sender/recipients, date and time, the number of media and the types of Support and Consulting Data they contain.<br>**Protection from Disruptions.** Microsoft uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference.<br>**Component Disposal.** Microsoft uses industry standard processes to delete Support and Consulting Data when it is no longer needed. |
| Communications and Operations Management | **Operational Policy**. Microsoft maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Support and Consulting Data.<br>**Data Recovery Procedures**<br>- On an ongoing basis, but in no case less frequently than once a week (unless no Support and Consulting Data has been updated during that period), Microsoft maintains multiple copies of Support and Consulting Data from which Support and Consulting Data can be recovered.<br>- Microsoft stores copies of Support and Consulting Data and data recovery procedures in a different place from where the primary computer equipment processing the Support and Consulting Data is located.<br>- Microsoft has specific procedures in place governing access to copies of Support and Consulting Data.<br>- Microsoft reviews data recovery procedures at least annually.<br>- Microsoft logs data restoration efforts, including the person responsible, the description of the restored data and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process.<br>**Malicious Software**. Microsoft has anti-malware controls to help avoid malicious software gaining unauthorized access to Support and Consulting Data, including malicious software originating from public networks.<br>**Data Beyond Boundaries**<br>- Microsoft encrypts, or enables Customer to encrypt, Support or Consulting Data that is transmitted over public networks.<br>- Microsoft restricts access to Support and Consulting Data in media leaving its facilities (e.g., through encryption).<br>**Event Logging**<br>- Microsoft logs the use of our data-processing systems.<br>- Microsoft logs access and use of information systems containing Support and Consulting Data, registering the access ID, time, authorization granted or denied, and relevant activity. |
| Access Control | **Access Policy**. Microsoft maintains a record of security privileges of individuals having access to Support and Consulting Data.<br>**Access Authorization**<br>- Microsoft maintains and updates a record of personnel authorized to access Microsoft systems that contain Support and Consulting Data.<br>- Microsoft deactivates authentication credentials that have not been used for a period of time not to exceed six months.<br>- Microsoft identifies those personnel who may grant, alter or cancel authorized access to data and resources.<br>- Microsoft ensures that where more than one individual has access to systems containing Support and Consulting Data, the individuals have separate identifiers/log-ins.<br>**Least Privilege**<br>- Technical support personnel are only permitted to have access to Support and Consulting Data when needed.<br>- Microsoft restricts access to Support and Consulting Data to only those individuals who require such access to perform their job function.<br>**Integrity and Confidentiality**<br>- Microsoft instructs Microsoft personnel to disable administrative sessions when leaving premises Microsoft controls or when computers are otherwise left unattended.<br>- Microsoft stores passwords in a way that makes them unintelligible while they are in force.<br>**Authentication**<br>- Microsoft uses industry standard practices to identify and authenticate users who attempt to access information systems.<br>- Where authentication mechanisms are based on passwords, Microsoft requires that the passwords are renewed regularly. |

| Domain | Practices |
|---|---|
| | - Where authentication mechanisms are based on passwords, Microsoft requires the password to be at least eight characters long.<br>- Microsoft ensures that de-activated or expired identifiers are not granted to other individuals.<br>- Microsoft monitors repeated attempts to gain access to the information system using an invalid password.<br>- Microsoft maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed.<br>- Microsoft uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage.<br>- **Network Design**. Microsoft has controls to avoid individuals assuming access rights they have not been assigned to gain access to Support and Consulting Data they are not authorized to access. |
| Information Security Incident Management | **Incident Response Process**<br>- Microsoft maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data.<br>- Microsoft tracks disclosures of Support and Consulting Data, including what data has been disclosed, to whom, and at what time.<br>**Service Monitoring**. Microsoft security personnel verify logs at least every six months to propose remediation efforts if necessary. |
| Business Continuity Management | - Microsoft maintains emergency and contingency plans for the facilities in which Microsoft information systems that process Support and Consulting Data Data are located.<br>- Microsoft's redundant storage and its procedures for recovering data are designed to attempt to reconstruct Support and Consulting Data in its original state from before the time it was lost or destroyed. |

### Microsoft Audits of Professional Services

- In addition to Clause 5 paragraph f and Clause 12 paragraph 2 of the Standard Contractual Clauses, Microsoft has established and agrees to maintain for Professional Services a data security policy that complies with the ISO 27001 standards for the establishment, implementation, control, and improvement of the Information Security Management System and the ISO/IEC 27002 code of best practices for information security management ("Information Security Policy"). On a confidential need-to-know basis, and subject to Customer's agreement to non-disclosure obligations Microsoft specifies, Microsoft will make the Information Security Policy available to Customer, along with other information reasonably requested by Customer regarding Microsoft security practices and policies. Customer is solely responsible for reviewing the Information Security Policy, making an independent determination as to whether the Information Security Policy meets Customer's requirements, and for ensuring that Customer's personnel and consultants follow the guidelines they are provided regarding data security.
- Microsoft will audit the security of the computers and computing environment that it uses in processing Support and Consulting Data (including personal data) while providing the Professional Services. This audit: (a) will be performed at least annually; (b) will be performed according to ISO 27001 standards; (c) will be performed by third party security professionals at Microsoft's selection and expense; (d) will result in the generation of an audit report ("Microsoft Audit Report"), which will be Microsoft's confidential information; and (e) may be performed for other purposes in addition to satisfying this Section (e.g., as part of Microsoft's regular internal security procedures or to satisfy other contractual obligations).
- If Customer requests in writing, Microsoft will provide Customer with a confidential summary of the Microsoft Audit Report ("Summary Report") so that Customer can reasonably verify Microsoft's compliance with the security obligations under this Addendum. The Summary Report is Microsoft confidential information.
- Customer agrees to exercise its audit right under the Standard Contractual Clauses by instructing Microsoft to execute the audit as described in Section 5(b)(i) – (iii). If Customer desires to change this instruction regarding exercising this audit right, then Customer has the right to change this instruction as mentioned in the Standard Contractual Clauses, which shall be requested in writing.
- Nothing in this Section 5(b) varies or modifies the Standard Contractual Clauses nor affects any supervisory authority's or data subject's rights under the Standard Contractual Clauses. Microsoft Corporation is an intended third-party beneficiary of this Section 5(b).

# Security Incident Notification

If Microsoft becomes aware of any unlawful access to any Support and Consulting Data stored on Microsoft's equipment or Microsoft facilities, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of Support and Consulting Data (each a "Security Incident"), Microsoft will promptly (a) notify Customer of the Security Incident; (b) investigate the Security Incident and provide Customer with detailed information about the Security Incident; and (c) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

Customer agrees that:

- An unsuccessful Security Incident will not be subject to this Section. An unsuccessful Security Incident is one that results in no unauthorized access to Support and Consulting Data or to any of Microsoft's equipment or facilities storing Support and Consulting Data, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond IP addresses or headers) or similar incidents; and
- Microsoft's obligation to report or respond to a Security Incident under this Section is not and will not be construed as an acknowledgement by Microsoft of any fault or liability with respect to the Security Incident.

Notification(s) of Security Incidents, if any, will be delivered to one or more of Customer's business contacts for the Professional Services by any means Microsoft selects, including via email.

# Attachment 1 – The Standard Contractual Clauses (Processors) for Support and Consulting Services

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, Customer (as data exporter) and Microsoft Corporation (as data importer, whose signature appears below), each a "party," together "the parties," have agreed on the following Contractual Clauses (the "Clauses" or "Standard Contractual Clauses") in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

**Clause 1: Definitions**

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

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

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) 'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

**Clause 2: Details of the transfer**

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 below which forms an integral part of the Clauses.

**Clause 3: Third-party beneficiary clause**

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

**Clause 4: Obligations of the data exporter**

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 below;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

**Clause 5: Obligations of the data importer**

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

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

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

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

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

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

**Clause 6: Liability**

1. The parties agree that any data subject who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

**Clause 7: Mediation and jurisdiction**

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

**Clause 8: Cooperation with supervisory authorities**

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

**Clause 9: Governing Law**

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

**Clause 10: Variation of the contract**

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

**Clause 11: Subprocessing**

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

**Clause 12: Obligation after the termination of personal data processing services**

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

**Appendix 1 to the Standard Contractual Clauses for Support and Consulting Services**

**Data exporter**: Customer is the data exporter. The data exporter is procuring professional IT support and consulting services as described in the applicable Enterprise Services Work Order.

**Data importer:** The data importer is Microsoft Corporation, a global producer of software and services.

**Data subjects**: Data subjects include the data exporter's representatives and end-users including employees, contractors, collaborators, and customers of the data exporter. Data subjects may also include individuals attempting to communicate or transfer personal information to users of the services provided by data importer.

**Categories of data**: The personal data transferred includes e-mail, documents and other data in an electronic form as necessary to provide the Professional Services.

**Processing operations**: The personal data transferred will be subject to the following basic processing activities:

**a. Duration and Object of Data Processing.** The duration of data processing shall be for the term designated under the applicable volume licensing agreement between the data exporter and the Microsoft entity to which these Standard Contractual Clauses are annexed ("Microsoft"). The objective of the data processing is the performance of the Professional Services.

**b. Scope and Purpose of Data Processing.** The scope and purpose of processing personal data is described in the Addendum and the Agreement.

**c. Support and Consulting Data Access.** For the term designated under the Agreement Microsoft will, at its election and as necessary under applicable law implementing Article 12(b) of the EU Data Protection Directive, either: (1) provide Customer with the ability to correct, delete, or block Support and Consulting Data, or (2) make such corrections, deletions, or blockages on Customer's behalf.

**d. Data Exporter's Instructions.** For Professional Services, data importer will only act upon data exporter's instructions as conveyed by Microsoft.

**e. Support and Consulting Data Deletion or Return.** Microsoft will delete or return all copies of Support and Consulting Data after the business purposes for which the Support and Consulting Data was collected or transferred have been fulfilled, or earlier upon Customer's written request.

**Subcontractors:** The data importer may hire other companies to provide limited services on data importer's behalf. Any such subcontractors will be permitted to obtain Support and Consulting Data only to deliver the services the data importer has retained them to provide, and they are prohibited from using Support and Consulting Data for any other purpose.

**Appendix 2 to the Standard Contractual Clauses for Support and Consulting Services**

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

1. **Personnel.** Data importer's personnel will not process Support and Consulting Data without authorization. Personnel are obligated to maintain the confidentiality of any Support and Consulting Data and this obligation continues even after their engagement ends.

2. **Data Privacy Contact.** The data privacy officer of the data importer can be reached at the following address:
Microsoft Corporation
Attn: Chief Privacy Officer
1 Microsoft Way
Redmond, WA 98052 USA

3. **Technical and Organization Measures.** The data importer has implemented and will maintain appropriate technical and organizational measures, internal controls, and information security routines intended to protect Support and Consulting Data, as defined in the Microsoft Professional Services Data Protection Addendum, against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction as follows: The technical and organizational measures, internal controls, and information security routines set forth in Exhibit 1 are hereby incorporated into this Appendix 2 by this reference and are binding on the data importer as if they were set forth in this Appendix 2 in their entirety.

Signature of Microsoft Corporation appears on the following page.

**Signing the Standard Contractual Clauses for Professional Services, Appendix 1 and Appendix 2 on behalf of the data importer:**

Signature:


**Anand Eswaran, Corporate Vice President**

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052 USA

# Attachment 2 – The Standard Contractual Clauses (Processors) for Consulting Services delivered by Global Delivery India

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, Customer (as data exporter) and Microsoft Global Services Center (India) Private Limited (as data importer, whose signature appears below), each a "party," together "the parties," have agreed on the following Contractual Clauses (the "Clauses" or "Standard Contractual Clauses") in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

**Clause 1: Definitions**

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

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

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) 'the subprocessor' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

**Clause 2: Details of the transfer**

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 below which forms an integral part of the Clauses.

**Clause 3: Third-party beneficiary clause**

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

**Clause 4: Obligations of the data exporter**

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 below;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

**Clause 5: Obligations of the data importer**

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

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

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

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

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

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

**Clause 6: Liability**

1. The parties agree that any data subject who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

**Clause 7: Mediation and jurisdiction**

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

**Clause 8: Cooperation with supervisory authorities**

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

**Clause 9: Governing Law**

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

**Clause 10: Variation of the contract**

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

**Clause 11: Subprocessing**

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

**Clause 12: Obligation after the termination of personal data processing services**

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

**Appendix 1 to the Standard Contractual Clauses for Consulting Services delivered by Global Delivery India**

**Data exporter**: Customer is the data exporter. The data exporter is procuring professional IT support and consulting services as described in the applicable Enterprise Services Work Order.

**Data importer:** The data importer is Microsoft Global Services Center (India) Private Limited, an affiliate of Microsoft Corporation that provides a global IT consulting services.

**Data subjects**: Data subjects include the data exporter's representatives and end-users including employees, contractors, collaborators, and customers of the data exporter. Data subjects may also include individuals attempting to communicate or transfer personal information to users of the services provided by data importer.

**Categories of data**: The personal data transferred includes e-mail, documents and other data in an electronic form as necessary to provide the Professional Services.

**Processing operations**: The personal data transferred will be subject to the following basic processing activities:

**a. Duration and Object of Data Processing.** The duration of data processing shall be for the term designated under the applicable volume licensing agreement between the data exporter and the Microsoft entity to which these Standard Contractual Clauses are annexed ("Microsoft"). The objective of the data processing is the performance of the Professional Services.

**b. Scope and Purpose of Data Processing.** The scope and purpose of processing personal data is described in the Addendum and the Agreement.

**c. Support and Consulting Data Access.** For the term designated under the Agreement Microsoft will, at its election and as necessary under applicable law implementing Article 12(b) of the EU Data Protection Directive, either: (1) provide Customer with the ability to correct, delete, or block Support and Consulting Data, or (2) make such corrections, deletions, or blockages on Customer's behalf.

**d. Data Exporter's Instructions.** For Professional Services, data importer will only act upon data exporter's instructions as conveyed by Microsoft.

**e. Support and Consulting Data Deletion or Return.** Microsoft will delete or return all copies of Support and Consulting Data after the business purposes for which the Support and Consulting Data was collected or transferred have been fulfilled, or earlier upon Customer's written request.

**Subcontractors:** The data importer may hire other companies to provide limited services on data importer's behalf. Any such subcontractors will be permitted to obtain Support and Consulting Data only to deliver the services the data importer has retained them to provide, and they are prohibited from using Support and Consulting Data for any other purpose.

**Appendix 2 to the Standard Contractual Clauses for Consulting Services delivered by Global Delivery India**

Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

1. **Personnel.** Data importer's personnel will not process Support and Consulting Data without authorization. Personnel are obligated to maintain the confidentiality of any Support and Consulting Data and this obligation continues even after their engagement ends.

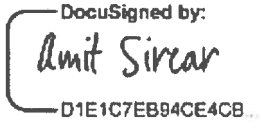
2. **Data Privacy Contact.** The data privacy officer of the data importer can be reached at the following address:
   Microsoft Global Services Center (India) Private Limited
   Attn: Ravi Piduri
   1 Microsoft Way
   Redmond, WA 98052 USA

3. **Technical and Organization Measures.** The data importer has implemented and will maintain appropriate technical and organizational measures, internal controls, and information security routines intended to protect Support and Consulting Data, as defined in the Microsoft Professional Services Data Protection Addendum, against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction as follows: The technical and organizational measures, internal controls, and information security routines set forth in Exhibit 1 are hereby incorporated into this Appendix 2 by this reference and are binding on the data importer as if they were set forth in this Appendix 2 in their entirety.

Signature of Microsoft Corporation appears on the following page.

**Signing the Standard Contractual Clauses for Consulting Services delivered from Global Delivery India, Appendix 1 and Appendix 2 on behalf of the data importer:**

Signature




**Amit Sircar, Vice President**

Microsoft Global Services Center (India) Private Limited
Building 1, Microsoft Campus, Gachibowli,
Hyderabad – 500032, India

# Attachment 3 – European Union General Data Protection Regulation Terms

**A. Definitions**

Terms used but not defined in these GDPR Terms, such as "personal data breach", "processing", "controller", "processor" and "data subject", will have the same meaning as set forth in Article 4 of the GDPR.

The following definition is also used in these GDPR Terms:

**"Subprocessors"** means the other processors that are used by Microsoft to process Personal Data.

**B. Roles and Scope**

**1.** These GDPR Terms apply to the processing of Personal Data, within the scope of the GDPR, by Microsoft on behalf of Customer.

**2.** For purposes of these GDPR Terms, Customer and Microsoft agree that Customer is the controller of Customer Personal Data and Microsoft is the processor of such data, except when Customer acts as a processor of Personal Data, in which case Microsoft is a subprocessor.

**3.** These GDPR Terms do not limit or reduce any data protection commitments Microsoft makes to Customer in the Support and Consulting Data Protection Addendum or other agreement between Microsoft and Customer.

**4.** These GDPR Terms do not apply where Microsoft is a controller of Personal Data.

**C. Relevant GDPR Obligations: Articles 28, 32, and 33**

**1.** Microsoft shall not engage another processor without prior specific or general written authorisation of Customer. In the case of general written authorisation, Microsoft shall inform Customer of any intended changes concerning the addition or replacement of other processors, thereby giving Customer the opportunity to object to such changes. (Article 28(2))

**2.** Processing by Microsoft shall be governed by these GDPR Terms under European Union (hereafter "Union") or Member State law and are binding on Microsoft with regard to Customer. The subject-matter and duration of the processing, the nature and purpose of the processing, the type of Personal Data, the categories of data subjects and the obligations and rights of the Customer are set forth in the Customer's volume licensing agreement, including these GDPR Terms. In particular, Microsoft shall:

**(a)** process the Personal Data only on documented instructions from Customer, including with regard to transfers of Personal Data to a third country or an international organisation, unless required to do so by Union or Member State law to which Microsoft is subject; in such a case, Microsoft shall inform Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

**(b)** ensure that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

**(c)** take all measures required pursuant to Article 32 of the GDPR;

**(d)** respect the conditions referred to in paragraphs 2 and 3 for engaging another processor;

**(e)** taking into account the nature of the processing, assist Customer by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR;

**(f)** assist Customer in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR, taking into account the nature of processing and the information available to Microsoft;

**(g)** at the choice of Customer, delete or return all the Personal Data to Customer after the end of the provision of services relating to processing, and delete existing copies unless Union or Member State law requires storage of the Personal Data;

**(h)** make available to Customer all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by Customer or another auditor mandated by Customer.

Microsoft shall immediately inform Customer if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions. (Article 28(3))

**3.** Where Microsoft engages another processor for carrying out specific processing activities on behalf of Customer, the same data protection obligations as set out in these GDPR Terms shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the GDPR. Where that other processor fails to fulfil its data protection obligations, Microsoft shall remain fully liable to the Customer for the performance of that other processor's obligations. (Article 28(4))

**4.** Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Customer and Microsoft shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

**(a)** the pseudonymisation and encryption of Personal Data;

**(b)** the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

**(c)** 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

**(d)** a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. (Article 32(1))

**5.** In assessing the appropriate level of security, account shall be taken of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed. (Article 32(2))

**6.** Customer and Microsoft shall take steps to ensure that any natural person acting under the authority of Customer or Microsoft who has access to Personal Data does not process them except on instructions from Customer, unless he or she is required to do so by Union or Member State law. (Article 32(4))

**7.** Microsoft shall notify Customer without undue delay after becoming aware of a personal data breach. (Article 33(2). Such notice will, at a minimum,

**(a)** 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;

**(b)** communicate the name and contact details of the data protection officer or other contact where more information can be obtained;

**(c)** describe the likely consequences of the personal data breach; and

**(d)** describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects. (Article 33(3))

# Appendix 1 – Additional GDPR Terms

**A. Subprocessors**

**1.** Customer consents to Microsoft engaging Subprocessors for the processing of Personal Data in accordance with these GDPR Terms.

**2.** Microsoft will ensure that Subprocessors are bound by written agreements that require them to provide at least the level of data protection required of Microsoft by these GDPR Terms.

**3.** A list of Microsoft's current Subprocessors for Support Services is available at: https://aka.ms/servicesapprovedsuppliers (such URL may be updated by Microsoft from time to time). At least 14 days before authorizing any new Subprocessor to access Personal Data, Microsoft will update the website and provide Customer with a mechanism to obtain notice of that update. Where Microsoft is a processor (and not a subprocessor), the following terms apply:

**(a)** If Customer does not approve of a new Subprocessor, then Customer may terminate any Work Order by providing, before the end of the notice period, written notice of termination in accordance with the termination provisions of the applicable Master Agreement, that includes an explanation of the grounds for non-approval.

**4.** A list of Microsoft's Subprocessors for Consulting Services is available upon request. If such list is requested, at least 14 days before authorizing any new Subprocessor to access Personal Data, Microsoft will update the list and provide Customer with a mechanism to obtain notice of that update.

**B. Assisting Customer Response to Requests from Data Subjects**

**1.** Microsoft will make available to Customer the Personal Data of its data subjects and the ability to fulfill data subject requests to exercise one or more of their rights under the GDPR in a manner consistent with Microsoft's role as a processor. Microsoft shall comply with reasonable requests by Customer to assist with Customer's response to such a data subject request.

**2.** If Microsoft receives a request from Customer's data subject to exercise one or more of its rights under the GDPR, Microsoft will redirect the data subject to make its request directly to Customer.

**C. Processing of Personal Data**

**1.** Customer's volume licensing agreement (including these GDPR Terms) are Customer's complete and final instructions to Microsoft for the processing of Personal Data.

**2.** Microsoft may also transfer Personal Data if required by applicable law.

**3.** Microsoft will ensure that its personnel engaged in the processing of Personal Data (i) will process Personal Data only on instructions from Customer, unless required to do so by Union, Member State, or other applicable law and (ii) have committed to maintain the confidentiality of any Personal Data even after their engagement ends.

**4.** The subject-matter of the processing is limited to Personal Data within the scope of the GDPR, and the duration of the processing shall be for the duration of the Customer's Professional Services engagement. The nature and purpose of the processing shall be to provide the Professional Services pursuant to Customer's volume licensing agreement. The types of Personal Data processed by the Professional Services include those expressly identified in Article 4 of the GDPR as well as other Personal Data submitted by Customer through the Professional Services engagement. The categories of data subjects are Customer's representatives and end users, such as employees, contractors, collaborators, and customers.

**5.** At the end of Customer's business relationship with Microsoft or on request, Microsoft shall delete or return Personal Data unless Union, Member State, or other applicable law requires storage of the Personal Data.

**D. Security**

Microsoft shall (i) maintain security practices and policies for the protection of Personal Data as set forth in the written data security policy (that policy an "Information Security Policy") for Professional Services, and (ii) subject to non-disclosure obligations, make the Information Security Policy available to Customer, along with descriptions of the security controls in place for Professional Services and other information reasonably requested by Customer regarding Microsoft security practices and policies.

**E. Personal Data Breach**

Microsoft shall make reasonable efforts to assist Customer in fulfilling Customer's obligation to notify the relevant supervisory authority and data subjects of a personal data breach under Articles 33 and 34 of the GDPR.

**F. Records of Processing Activities**

Microsoft shall maintain all records required by Article 30(2) of the GDPR and, to the extent applicable to the processing of Personal Data on behalf of Customer, make them available to Customer upon request.

**G. Modification, Supplementation, and Term**

**1.** Microsoft may modify or supplement these GDPR Terms, with notice to Customer, (i) if required to do so by a supervisory authority or other government or regulatory entity, (ii) if necessary to comply with applicable law, (iii) to implement standard contractual clauses laid down by the European Commission or (iv) to adhere to an approved code of conduct or certification mechanism approved or certified pursuant to Articles 40, 42 and 43 of the GDPR.

**2.** Without prejudice to these GDPR Terms, Microsoft may from time to time provide additional information and detail about how it will execute these GDPR Terms in its technical, privacy, or policy documentation.

**3.** These GDPR Terms become effective upon the later of (a) the start of enforcement of the GDPR or (b) Microsoft's provision of Professional Services for which Microsoft is a processor or subprocessor.