Volume Licensing

Online Services Terms
April 2020

Microsoft

Table of Contents

Introduction

The parties agree that these Online Services Terms govern Customer's use of the Online Services and that the DPA (defined below) sets forth their obligations with respect to the processing and security of Customer Data and Personal Data by the Online Services. The parties also agree that, unless a separate Professional Services agreement exists, these Online Services Terms govern the provision of Professional Services, including but not limited to the terms in Attachment 1 and terms in the DPA for the processing and security of Professional Services Data and Personal Data in connection with that provision. Separate terms, including different privacy and security terms, govern Customer's use of Non-Microsoft Products (as defined below). In the event of any conflict or inconsistency between the DPA and any other terms in Customer's volume licensing agreement (including the Product Terms or the Online Services Terms), the DPA shall prevail.

Service Level Agreements
Most Online Services offer a Service Level Agreement (SLA). For more information regarding the Online Services SLAs, please refer to http://microsoft.com/licensing/contracts.

Applicable Online Services Terms and Updates
When Customer renews or purchases a new subscription to an Online Service, the then-current Online Services Terms will apply and will not change during Customer's subscription for that Online Service. When Microsoft introduces features, supplements or related software that are new (i.e., that were not previously included with the subscription), Microsoft may provide terms or make updates to the Online Services Terms that apply to Customer's use of those new features, supplements or related software.

Electronic Notices
Microsoft may provide Customer with information and notices about Online Services electronically, including via email, through the portal for the Online Service, or through a web site that Microsoft identifies. Notice is given as of the date it is made available by Microsoft.

Prior Versions
The Online Services Terms provides terms for Online Services that are currently available. For earlier versions of the Online Services Terms, Customer may refer to http://go.microsoft.com/?linkid=9840733 or contact its reseller or Microsoft Account Manager.

Clarifications and Summary of Changes

Additions	Deletions
GitHub Learning Lab for Organizations	
GitHub One	

Online Service Specific Terms
Microsoft 365 – Unattended License: Added new entry describing the use terms for the new Microsoft 365 – Unattended License for Unattended Bots.
GitHub Offerings: Added terms for GitHub One – Premium Support for GitHub Enterprise.
Microsoft Threat Protection: Added a new entry for Microsoft Threat Protection that includes service specific privacy terms.

Attachment 1 – Notices
Core Online Services: Added Norway as a geographic region for Customer Data at Rest for Office 365 Services.

Attachment 2 – Subscription License Suites
Subscription License Suites: Updated table to include new/updated Microsoft 365 F1 offer.

Table of Contents / General Terms

Definitions

If any of the terms below are not defined in Customer's volume licensing agreement, they have the definitions below.

"Core Online Services" means those Online Services listed as Core Online Services in Attachment 1.

"Customer Data" means all data, including all text, sound, video, or image files, and software, that are provided to Microsoft by, or on behalf of, Customer through use of the Online Service. Customer Data does not include Professional Services Data.

"Data Protection Addendum" (DPA) means the Microsoft Online Services Data Protection Addendum published at https://aka.ms/DPA.

"External User" means a user of an Online Service that is not an employee, onsite contractor, or onsite agent of Customer or its Affiliates.

"Instance" means an image of software that is created by executing the software's setup or install procedure or by duplicating such an image.

"Licensed Device" means a single physical hardware system, dedicated to Customer's use, to which a license is assigned. Any dedicated device that is under the management or control of an entity other than Customer or one of its Affiliates is subject to the Outsourcing Software Management clause of the Product Terms located at http://go.microsoft.com/?linkid=9839207. For purposes of this definition, a hardware partition or blade is considered to be a separate device.

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

"Network Server" means a physical hardware server solely dedicated to Customer use and provides resource assistant to computers in a network. Any dedicated server that is under the management or control of an entity other than Customer or one of its Affiliates is subject to the Outsourcing Software Management clause of the Product Terms. The Product Terms is located at http://go.microsoft.com/?linkid=9839207

"Non-Microsoft Product" means any third-party-branded software, data, service, website or product, unless incorporated by Microsoft in an Online Service.

"Online Service" means a Microsoft-hosted service to which Customer subscribes under a Microsoft volume licensing agreement, including any service identified in the Online Services section of the Product Terms. It does not include software and services provided under separate license terms (such as via gallery, marketplace, console, or dialog). The Product Terms is located at http://go.microsoft.com/?linkid=9839207.

"Operating System Environment" (OSE) means all or part of an operating system Instance, or all or part of a virtual (or otherwise emulated) operating system Instance, that enables separate machine identity (primary computer name or similar unique identifier) or separate administrative rights, and Instances of applications, if any, configured to run on all or part of that operating system Instance. There are two types of OSEs, physical and virtual. A physical hardware system can have one physical OSE and/or one or more virtual OSEs. The operating system Instance used to run hardware virtualization software or to provide hardware virtualization services is considered part of the physical OSE.

"OST" means these Online Services Terms.

"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.

"Previews" means preview, beta or other pre-release features, data center locations, and services offered by Microsoft for optional evaluation.

"Professional Services" means Microsoft technical support and consulting services (e.g., for data migration) related to any Online Service.

"Professional Services Data" means all data, including all text, sound, video, image files or software, that are provided to Microsoft, by or on behalf of a Customer (or that Customer authorizes Microsoft to obtain from an Online Service) or otherwise obtained or processed by or on behalf of Microsoft through an engagement with Microsoft to obtain Professional Services. Professional Services Data includes Support Data.

"SL" means subscription license.

"Subprocessor" means other processors used by Microsoft to process data.

"Support 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 technical support for Online Services covered under this agreement. Support Data is a subset of Professional Services Data.

General Terms

Licensing the Online Services

Customer must acquire and assign the appropriate subscription licenses required for its use of each Online Service. Each user that accesses the Online Service must be assigned a User SL or access the Online Service only through a device that has been assigned a Device SL, unless specified otherwise in the Online Service-specific Terms. Attachment 2 describes SL Suites that also fulfill requirements for User SLs. Customer has no right to use an Online Service after the SL for that Online Service ends.

License Reassignment

Most, but not all, SLs may be reassigned. Except as permitted in this paragraph or in the Online Service-specific Terms, Customer may not reassign an SL on a short-term basis (i.e., within 90 days of the last assignment). Customer may reassign an SL on a short-term basis to cover a user's absence or the unavailability of a device that is out of service. Reassignment of an SL for any other purpose must be permanent. When Customer reassigns an SL from one device or user to another, Customer must block access and remove any related software from the former device or from the former user's device.

Multiplexing

Hardware or software that Customer uses to pool connections; reroute information; reduce the number of devices or users that directly access or use the Online Service (or related software); or reduce the number of OSEs, devices or users the Online Service directly manages (sometimes referred to as "multiplexing" or "pooling") does not reduce the number of licenses of any type (including SLs) that Customer needs.

Using the Online Services

Customer may use the Online Services and related software as expressly permitted in Customer's volume licensing agreement. Microsoft reserves all other rights.

Acceptable Use Policy

Neither Customer, nor those that access an Online Service through Customer, may use an Online Service:

- in a way prohibited by law, regulation, governmental order or decree;
- to violate the rights of others;
- to try to gain unauthorized access to or disrupt any service, device, data, account or network;
- to spam or distribute malware;
- in a way that could harm the Online Service or impair anyone else's use of it;
- in any application or situation where failure of the Online Service could lead to the death or serious bodily injury of any person, or to severe physical or environmental damage; or
- to assist or encourage anyone to do any of the above.

Violation of the Acceptable Use Policy in this section may result in suspension of the Online Service. Microsoft will suspend the Online Service only to the extent reasonably necessary. Unless Microsoft believes an immediate suspension is required, Microsoft will provide reasonable notice before suspending an Online Service.

Data Protection and Security

The terms of the DPA apply to Online Services except for Online Services listed in Attachment 1. For Core Online Services, Online Service-specific details on security practices and location of Customer Data at rest are in Attachment 1.

Use of Software with the Online Service

Customer may need to install certain Microsoft software to use the Online Service. If so, the following terms apply:

Microsoft Software License Terms

Customer may install and use the software only for use with the Online Service. The Online Service-specific Terms may limit the number of copies of the software Customer may use or the number of devices on which Customer may use it. Customer's right to use the software begins when the Online Service is activated and ends when Customer's right to use the Online Service ends. Customer must uninstall the software when Customer's right to use it ends. Microsoft may disable it at that time.

Validation, Automatic Updates, and Collection for Software

Microsoft may automatically check the version of any of its software. Devices on which the software is installed may periodically provide information to enable Microsoft to verify that the software is properly licensed. This information includes the software version, the end user's user account, product ID information, a machine ID, and the internet protocol address of the device. If the software is not properly licensed, its functionality will be affected. Customer may only obtain updates or upgrades for the software from Microsoft or authorized sources. By using

the software, Customer consents to the transmission of the information described in this section. Microsoft may recommend or download to Customer's devices updates or supplements to this software, with or without notice. Some Online Services may require, or may be enhanced by, the installation of local software (e.g., agents, device management applications) ("Apps"). The Apps may collect Diagnostic Data (as defined in the DPA) about the use and performance of the Apps, which may be transmitted to Microsoft, to the extent any Personal Data is contained therein, and used for the purposes described in the DPA.

Third-party Software Components

The software may contain third party software components. Unless otherwise disclosed in that software, Microsoft, not the third party, licenses these components to Customer under Microsoft's license terms and notices.

Technical Limitations

Customer must comply with, and may not work around, any technical limitations in an Online Service that only allow Customer to use it in certain ways. Customer may not download or otherwise remove copies of software or source code from an Online Service except as explicitly authorized.

Import/Export Services

Customer's use of any Import/Export Service is conditioned upon its compliance with all instructions provided by Microsoft regarding the preparation, treatment and shipment of physical media containing its data ("storage media"). Customer is solely responsible for ensuring the storage media and data are provided in compliance with all laws and regulations. Microsoft has no duty with respect to the storage media and no liability for lost, damaged or destroyed storage media. All storage media shipped to Microsoft must be shipped DAP Microsoft DCS Data Center (INCOTERMS 2010). Storage media shipped to Customer will be shipped DAP Customer Dock (INCOTERMS 2010).

Font Components

While Customer uses an Online Service, Customer may use the fonts installed by that Online Service to display and print content. Customer may only embed fonts in content as permitted by the embedding restrictions in the fonts and temporarily download them to a printer or other output device to print content.

Changes to and Availability of the Online Services

Microsoft may make commercially reasonable changes to each Online Service from time to time. Microsoft may modify or terminate an Online Service in any country where Microsoft is subject to a government regulation, obligation or other requirement that (1) is not generally applicable to businesses operating there, (2) presents a hardship for Microsoft to continue operating the Online Service without modification, and/or (3) causes Microsoft to believe these terms or the Online Service may conflict with any such requirement or obligation. If Microsoft terminates an Online Service for regulatory reasons, Customers will receive a credit for any amount paid in advance for the period after termination.

Availability, functionality, and language versions for each Online Service may vary by country. For information on availability, Customer may refer to https://go.microsoft.com/fwlink/?linkid=870295.

Other

Non-Microsoft Products

Microsoft may make Non-Microsoft Products available to Customer through Customer's use of the Online Services (such as through a store or gallery, or as search results) or a Microsoft online store (such as the Microsoft Store for Business or Microsoft Store for Education). If Customer installs or uses any Non-Microsoft Product with an Online Service, Customer may not do so in any way that would subject Microsoft's intellectual property or technology to obligations beyond those expressly included in Customer's volume licensing agreement. For Customer's convenience, Microsoft may include charges for certain Non-Microsoft Product as part of Customer's bill for Online Services. Microsoft, however, assumes no responsibility or liability whatsoever for any Non-Microsoft Product. Customer is solely responsible for any Non-Microsoft Product that it installs or uses with an Online Service or acquires or manages through a Microsoft online store. Customer's use of any Non-Microsoft Product shall be governed by the license, service, and/or privacy terms between Customer and the publisher of the Non-Microsoft Product (if any).

Previews

PREVIEWS ARE PROVIDED "AS-IS," "WITH ALL FAULTS," AND "AS AVAILABLE," as described herein. Previews are not included in the SLA for the corresponding Online Service, and may not be covered by customer support. We may change or discontinue Previews at any time without notice. We may also choose not to make a Preview service generally commercially available.

Unless otherwise noted in a separate agreement, Previews are not included in the SLA for the corresponding Online Service.

Providing "Feedback" (suggestions, comments, feedback, ideas, or know-how, in any form) to Microsoft about Preview services is voluntary. Microsoft is under no obligation to post or use any Feedback. By providing Feedback to Microsoft, Customer (and anyone providing Feedback through Customer) irrevocably and perpetually grant to Microsoft and its Affiliates, under all of its (and their) owned or controlled intellectual property rights, a worldwide, non-exclusive, fully paid-up, royalty-free, transferable, sub-licensable right and license to make, use, reproduce, prepare derivative works based upon, distribute, publicly perform, publicly display, transmit, and otherwise commercialize the Feedback (including by combining or interfacing products, services or technologies that depend on or incorporate Feedback with other products, services or technologies of Microsoft or others), without attribution in any way and for any purpose.

Customer warrants that 1) it will not provide Feedback that is subject to a license requiring Microsoft to license anything to third parties because Microsoft exercises any of the above rights in Customer's Feedback; and 2) it owns or otherwise controls all of the rights to such Feedback and that no such Feedback is subject to any third-party rights (including any personality or publicity rights).

Azure Active Directory, Free Edition

As described in https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis, most Online Services include an instance of Azure Active Directory, a cloud-based user authentication capability ("Azure AD Free"). After Customer configures and uses the first such Online Service, that instance of Azure AD Free, as configured by Customer for its users, may power the user authentication features for each later-acquired subscription of an Online Service.

Customer's instance of Azure AD Free will also enable authenticated users to interact with Microsoft or a third party in contexts outside of the Online Services ("Other AD-dependent Services"), specifically where Microsoft or that third party requires an Azure Active Directory user account. With respect to the operation of Azure AD Free for Other AD-dependent Services, Microsoft remains a data processor, and this use of Azure AD Free constitutes Customer's authoritative instruction to Microsoft that such use is permitted. With respect to the operation of the Other AD-dependent Service, refer to its applicable agreement and privacy policy to determine the role of the provider of the Other AD-dependent Service.

Competitive Benchmarking

If Customer offers a service competitive to an Online Service, by using the Online Service, Customer agrees to waive any restrictions on competitive use and benchmark testing in the terms governing its competitive service. If Customer does not intend to waive such restrictions in its terms of use, Customer is not allowed to use the Online Service.

Government Customers

If Customer is a government entity, then the following terms apply to any Online Service provided at no charge to Customer:

i. Microsoft waives any and all entitlement to compensation from Customer for the Online Service.
ii. In compliance with applicable laws and regulations, Microsoft and Customer acknowledge that the Online Services are for the sole benefit and use of Customer and not provided for the personal use or benefit of any individual government employee.

German Online Services

Use of the German Online Services is further subject to the offer-specific terms available at https://aka.ms/MCAGermanSupplement.

Online Service Specific Terms

In addition to the General Terms for Online Services above, the following Online Service -specific terms apply to the listed Online Services. In the event of any conflict or inconsistency between the General Terms and the Online Service-specific terms, the Online Service-specific terms shall prevail as to the applicable Online Services. If an Online Service is not listed below, it does not have any Online Service-specific terms.

Microsoft Azure Services

Notices

The Bing Maps, Professional Services, Azure Media Services H.265/HEV Encoding, Adobe Flash Player, H.264/AVC Visual Standard, VC-1 Video Standard, and MPEG-4 Part 2 Visual Standard and MPEG-2 Video Standard Notices in Attachment 1 apply.

Service Level Agreement

Refer to http://azure.microsoft.com/support/legal/sla/.

Definitions

"Azure Government Services" means one or more of the services or features Microsoft makes available to Customer as Government Community Cloud Services in the "US Gov" regions identified at http://azure.microsoft.com/en-us/regions/#services.

"Bing Search Services" means the Bing Custom Search, Bing Local Business Search, Entity Search, Image Search, News Search, Video Search, Visual Search, Web Search, Spell Check, and Autosuggest APIs, and any other APIs identified at https://aka.ms/r1j7jq.

"Bing Search Services Data" means Customer Data that are provided to Microsoft by, or on behalf of, Customer through use of the Bing Search Services.

"Customer Solution" means an application or any set of applications that adds primary and significant functionality to the Microsoft Azure Services and that is not primarily a substitute for the Microsoft Azure Services.

"Microsoft Azure Services" means the Microsoft services and features identified at http://azure.microsoft.com/services/, except those licensed separately. "Microsoft Azure Services" includes any open source components incorporated by Microsoft in those services and features.

"Microsoft Translator" means Translator Text API and/or Translator Speech API offered by Microsoft as a cloud based machine translation service.

Limitations

Customer may not

- resell or redistribute the Microsoft Azure Services, or
- allow multiple users to directly or indirectly access any Microsoft Azure Service feature that is made available on a per user basis (e.g., Active Directory Premium). Specific reassignment terms applicable to a Microsoft Azure Service feature may be provided in supplemental documentation for that feature.

Retirement of Services or Features

Microsoft will provide Customer with 12 months' notice before removing any material feature or functionality or discontinuing a service, unless security, legal or system performance considerations require an expedited removal. This does not apply to Previews

Data Retention after Expiration or Termination

The expiration or termination of Customer's Online Service subscription will not change Customer's obligation to pay for hosting of Customer Data during any Extended Term.

Hosting Exception

Customer may create and maintain a Customer Solution and, despite anything to the contrary in Customer's volume licensing agreement, combine Microsoft Azure Services with Customer Data owned or licensed by Customer or a third party, to create a Customer Solution using the Microsoft Azure Service and the Customer Data together. Customer may permit third parties to access and use the Microsoft Azure Services in connection with the use of that Customer Solution. Customer is responsible for that use and for ensuring that these terms and the terms and conditions of Customer's volume licensing agreement are met by that use.

Use of Software within Microsoft Azure

For Microsoft software available within a Microsoft Azure Service, Microsoft grants Customer a limited license to use the software only within the Microsoft Azure Service.

Data Center Availability
Usage of data centers in certain regions may be restricted to Customers located in or near that region. For information on service availability by region, please refer to http://azure.microsoft.com/en-us/regions.

Sharing
The Microsoft Azure Services may provide the ability to share a Customer Solution and/or Customer Data with other Azure users and communities, or other third parties. If Customer chooses to engage in such sharing, Customer agrees that it is giving a license to all authorized users, including the rights to use, modify, and repost its Customer Solution and/or the Customer Data, and Customer is allowing Microsoft to make them available to such users in a manner and location of its choosing.

Marketplace
Microsoft Azure enables Customer to access or purchase products and services which are optimized for use with Azure through features such as the Microsoft Azure Marketplace and the Virtual Machine Gallery, subject to separate terms available at http://azure.microsoft.com/en-us/support/legal/store-terms.

Table of Contents / General Terms

Azure DevTest Labs

Secrets in DevTest Labs
Azure DevTest Labs automatically creates a key vault when a user saves a secret for the first time. Customer may not use this key vault to store anything other than DevTest Lab related passwords, SSH keys, or personal access tokens.

Table of Contents / General Terms

Azure Lab Services

While Microsoft provides Azure Lab Services to Customer, as between Customer and Microsoft, Customer is the sole provider of related services to Customer's end users and shall have sole and exclusive responsibility to end users, including any support obligations. Customer's end users are not a party to any agreement with Microsoft regarding the services.

Notification; Liability; Bar on Actions Against Microsoft
Customer will notify Microsoft promptly of any incidents that could have an impact on Microsoft such as a data breach, password issues, end user complaint(s), loss of user data, or intellectual property or privacy claims.

Customer acknowledges and agrees that Microsoft has no obligation or liability to Customer or any end user for the end user's usage of the service.

By using the service, an end user may not bring any action against Microsoft in relation to the services. If any end user does bring an action against Microsoft, the Indemnification provision in this section applies.

Indemnification
Customer agrees to hold harmless and indemnify Microsoft from and against any claim by an end user, third party, and/or regulatory authority in connection with the service provided to end users. Customer shall pay any resulting judgment, or settlement, and all costs, including reasonable attorney's fees, and expenses related thereto.

End User Terms
In order to provide the services to end users, Customer and Customer's end users must validly agree to a binding, written agreement that contain the substance of the following requirements:

Statement of Relationship: Customer is the sole provider of the services. Customer is responsible for providing any support to end users. The services will be provided by Customer to Customer's end users under your terms of use and privacy policy.

Compliance; Acceptable Use: Customer is solely responsible for ensuring compliance with all applicable laws, including, but not limited GDPR, with respect to Customer's provision and end users' use of the service. In addition, for clarity and without limiting the Acceptable Use Policy, Customer and Customer's end users may not use Azure Lab Services to facilitate or engage in cryptocurrency mining. Violation of this prohibition may result in suspension of the service, as set forth in the Acceptable Use Policy.

Disclaimer of Warranties: Customer will disclaim any and all warranties in connection with the services, and Customer will disclaim the same with respect to Microsoft.

Limitation of Liability and Exclusion of Damages: Customer will disclaim liability and exclude damages in a way that is consistent with the provisions of any applicable agreement(s) between Customer and Microsoft.

Updates
Customer is responsible for updating the virtual machines (VMs) in Customer's portfolio. Notwithstanding the foregoing, Microsoft may, but is not obligated to, take any action it deems reasonable in its business judgment with respect to the VMs in your portfolio, including applying any updates or other changes generally applicable to the services.

Table of Contents / General Terms

Azure Machine Learning service

NVIDIA Components
Azure Machine Learning service may include NVIDIA Corporation's CUDA Toolkit, Tesla drivers, cuDNN, DIGITS, NCCL, and TensorRT (the "NVIDIA Components"), Customer agrees that its use of NVIDIA Components is governed by the NVIDIA Cloud End User License Agreement for Compute at https://go.microsoft.com/fwlink/?linkid=874330.

Table of Contents / General Terms

Azure Maps

Navigation restrictions
Customer may not use Azure Maps to enable turn-by-turn navigation functionality in any application.

Database restrictions
Customer may not use Azure Maps or any part thereof to create a competing database or service, or a derived database populated wholly or partially with Customer's data and/or data supplied or created by any third party.

Customer will not use the data delivered by the Azure Maps in combination with any other third-party database, except that Customer may layer onto the data of a type not already included within the Service (such as your proprietary content) or of which Microsoft otherwise licenses.

API Results
Customer may not cache or store information delivered by the Azure Maps API including but not limited to geocodes and reverse geocodes, map data tiles and route information (the "Results") for the purpose of scaling such Results to serve multiple users, or to circumvent any functionality in Azure Maps.

Caching and storing Results is permitted where the purpose of caching is to reduce latency times of Customer's application. Results may not be stored for longer than: (i) the validity period indicated in returned headers; or (ii) 6 months, whichever is the shortest.

Customer may not display any Results on any third-party content or geographical map database.

Map Data
Use of content displaying the TomTom copyright notice must be in accordance with restrictions set forth in the TomTom Licensing Third Party Product Terms and EULA (https://www.tomtom.com/en_GB/thirdpartyproductterms/). Azure Maps uses Bing Imagery which subject to the Bing Maps Notice in Attachment 1.

User region parameter
User region parameter in Azure Maps must be used in compliance with applicable laws, including those regarding mapping, of the country where maps, images and other data and third party content that Customer is authorized to access via Azure Maps is made available.

No warranty for accuracy
Microsoft and its suppliers make no warranty that the maps, images, data or any content delivered by Azure Maps will be accurate or complete.

Copyright
Customer may not remove, obscure, mask or change any logo and/or copyright notice placed on or automatically generated by Azure Maps.

Table of Contents / General Terms

Azure Stack Hub

Azure Stack Hub Privacy
The Microsoft Privacy Statement located at https://go.microsoft.com/fwlink/?LinkId=521839 applies to Customer's use of Azure Stack Hub. If a Microsoft Cloud Agreement or Microsoft Customer Agreement Customer uses Azure Stack Hub software or services that are hosted by a Reseller, such use will be subject to Reseller's privacy practices, which may differ from Microsoft's.

To the extent Microsoft is a processor or subprocessor of personal data in connection with Azure Stack Hub, Microsoft makes to all customers, the commitments in (a) the "Processing of Personal Data; GDPR" provision of the DPA and (b) the European Union General Data Protection Regulation Terms in Attachment 3 of the DPA.

Use of Azure Stack Hub
Customer may use Azure Stack Hub only on the hardware on which it is preinstalled.

Use of the Default Provider Subscription
The subscription created for the system administrator during the Azure Stack Hub deployment process (the default provider subscription) may be used solely to deploy and manage the Azure Stack Hub infrastructure; it may not be used to run any workload that does not deploy or manage Azure Stack Hub infrastructure (e.g. it may not be used to run any application workloads).

Table of Contents / General Terms

Bing Search Services

Bing Search Services Use and Display Requirements
Customer must comply with use and display requirements for the Bing Search Services which are available at https://aka.ms/r1j7jq. Customer must use results it obtains through the Bing Search Services only in Internet Search Experiences (as defined in the use and display requirements) and must not cache or copy results. The results Customer obtains through the Bing Search Services are not Products, Fixes, or Services Deliverables.

Bing Search Services Privacy
The Microsoft Privacy Statement located at https://go.microsoft.com/fwlink/?LinkId=521839 applies to Customer's use of Bing Search Services, except that this Bing Search Services section of the Online Services Terms controls to the extent it conflicts with the Microsoft Privacy Statement.

Use of Bing Search Services Data
Customer is solely responsible for the content of all Bing Search Services Data.

Microsoft may process Bing Search Services Data solely to: (i) provide Cognitive Services to Customer; and (ii) improve Microsoft products and services. Solely for such processing, Microsoft may collect, retain, use, reproduce, and create derivative works of, Bing Search Services Data and Customer grants Microsoft a limited nonexclusive irrevocable worldwide license to do so. Customer will secure and maintain all rights necessary for Microsoft to process Bing Search Services Data as described in this paragraph without violating the rights of any third party or otherwise obligating Microsoft to Customer or to any third party.

This Use of Bing Search Services Data section of the Online Services Terms will survive termination or expiration of Customer's volume licensing agreement. As between the parties, Customer retains all right, title and interest in and to Bing Search Services Data. Microsoft acquires no rights in Bing Search Services Data, other than the rights Customer grants to Microsoft in this Use of Bing Search Services Data section. This paragraph does not affect Microsoft's rights in software or services Microsoft licenses to Customer.

Application of Data Protection Terms to Bing Search Services
Only the following sections of the DPA apply to the Bing Search Services: Data Transfers, Use of Subcontractors, and How to Contact Microsoft. These sections do not apply to Previews of the listed services.

GDPR Terms do not apply to Bing Search Services:
The GDPR Terms (as defined in the DPA) do not apply to the Bing Search Services.

Precedence:
This Bing Search Services section controls to the extent there is any conflict with other parts of the OST or DPA.

Table of Contents / General Terms

Cognitive Services

Limit on Customer use of service output
Customer will not, and will not allow third parties to use Cognitive Services or data from Cognitive Services to create, train, or improve (directly or indirectly) a similar or competing product or service.

Microsoft Translator Attribution
When displaying automatic translations performed by Microsoft Translator, Customer will provide reasonably prominent notice that the text has been automatically translated by Microsoft Translator.

Cognitive Services in Containers

Cognitive Services features that are available in containers are designed to connect to a billing endpoint. The containers and the billing endpoint are licensed to Customer under this agreement as Online Services. The containers are needed to use the billing endpoint and are also subject to the terms for use of software with an Online Service in this agreement. The containers include material that is confidential and proprietary to Microsoft. Customer agrees to keep that material confidential and to promptly notify Microsoft of any possible misuse. The containers are not subject to the DPA because the operating environment of the containers is not under Microsoft's control. Customer must configure the containers it uses to communicate with the billing endpoint so that the billing endpoint meters all use of those containers. Provided Customer enables such metering and subject to any applicable transaction limits, Customer may install and use any number of containers (1) on Customer's hardware devices that are dedicated to Customer's exclusive use, and (2) in Customer's Microsoft Azure Service accounts.

Inactive Cognitive Services Configurations and Custom Models

For the purposes of data retention and deletion, a Cognitive Services configuration or custom model that has been inactive may at Microsoft's discretion be treated as an Online Service for which the Customer's subscription has expired. A configuration or custom model is inactive if for 90 days (1) no calls are made to it; (2) it has not been modified and does not have a current key assigned to it and; (3) Customer has not signed in to it.

Table of Contents / General Terms

Microsoft Genomics

Microsoft Genomics Privacy

The Microsoft Privacy Statement located at https://go.microsoft.com/fwlink/?LinkId=521839 applies to Customer's use of Microsoft Genomics, except that this Microsoft Genomics section controls to the extent it conflicts with the Microsoft Privacy Statement.

Broad License Terms

Microsoft Genomics includes access to the Genetic Analysis Toolkit (GATK) from the Broad Institute, Inc. ("Broad"). Use of the GATK and any related documentation as part of Microsoft Genomics is also subject to Broad's GATK End User License Agreement ("Broad EULA" located here https://software.broadinstitute.org/gatk/eula/index?p=Azure).

Microsoft may collect and share with Broad certain statistical and technical information regarding Customer's usage of the GATK. Customer authorizes Microsoft to report to Broad Customer's status as a user of the GATK in Microsoft Genomics.

No Medical Use

Microsoft Genomics is not a medical device and outputs generated from its use are not intended to be statements of fact, nor are they to be used as a substitute for medical judgment, advice, diagnosis or treatment of any disease or condition.

Table of Contents / General Terms

Visual Studio App Center

Visual Studio App Center Test Privacy and Security Terms

The privacy statement located at https://aka.ms/actestprivacypolicy applies to Customer's use of Visual Studio App Center Test. Customer may not use Visual Studio App Center Test to store or process Personal Data. Please refer to the Product documentation for more information.

Use for Development and Testing

Customer may only access and use Visual Studio App Center to develop and test Customer's application(s). Only one Licensed User may access a virtual machine provided by Visual Studio App Center at any time.

Authorized Developer

Customer appoints Microsoft as its authorized developer with respect to Apple software included in Visual Studio App Center. Microsoft is responsible for complying with the terms for any such software included in Visual Studio App Center and will keep confidential any confidential information of Apple accessed as part of Visual Studio App Center.

Third Party Repository Service Access

If Customer grants Microsoft access to its third-party repository service account(s), Customer authorizes Microsoft to scan the account(s), including the contents of Customer's public and private repositories.

Table of Contents / General Terms

Microsoft Azure Plans

Notices
The Bing Maps Notices in Attachment 1 apply.

Subscription License Suites
In addition to User SLs, refer to Attachment 2 for other SLs that fulfill requirements for Azure Active Directory Premium, Azure Advanced Threat Protection for Users, Azure Information Protection, and Microsoft Intune.

Azure Active Directory Basic

Customer may, using Single Sign-On, pre-integrate up to 10 SAAS Applications/Custom Applications per User SL. All Microsoft as well as third party applications count towards this application limit.

Table of Contents / General Terms

Azure Active Directory Premium

Customer may, using Single Sign-On, pre-integrate SaaS Applications/Custom Applications. Customer may not copy or distribute any data set (or any portion of a data set) included in the Microsoft Identity Manager software that is included with a Microsoft Azure Active Directory Premium (P1 and P2) User SL.

External User Allowance
For each User SL (or equivalent Subscription License Suite) Customer assigns to a user, Customer may also permit up to five additional External Users to access the corresponding Azure Active Directory service level.

Table of Contents / General Terms

Azure Information Protection Premium

Notices
The Bing Maps Notices in Attachment 1 applies. Any deployment services provided to Customer are subject to the Professional Services Notice in Attachment 1.

Table of Contents / General Terms

Microsoft Dynamics 365 Services

Notices
The Bing Maps and Professional Services Notices in Attachment 1 apply. Any onboarding, migration, or deployment services provided to Customer are subject to the Professional Services Notice in Attachment 1. In addition, Azure Media Services H.265/HEVC Encoding, H.264/AVC Visual Standard, VC-1 Video Standard, and MPEG-4 Part 2 Visual Standard and MPEG-2 Video Standard Notices in Attachment 1 apply only to Dynamics 365 Commerce.

External Users
External Users of Dynamics 365 Services do not need a SL to access the Online Service. This exemption does not apply to (1) contractors or agents of Customer or its Affiliates, or (2) External Users using Dynamics 365 client software with Dynamics 365 Services other than services or components included in Dynamics 365 Supply Chain Management, Dynamics 365 Finance, Dynamics 365 Commerce, or Dynamics 365 Human Resources.

Administration Portal
Customers with Dynamics 365 Supply Chain Management, Dynamics 365 Finance, Dynamics 365 Commerce, or Dynamics 365 Human Resources SLs may deploy and manage the Online Service through Microsoft Dynamics Lifecycle Services (or its successor), which is subject to separate terms.

Mixed deployments of Dynamics 365 services
Customers may mix (i) Dynamics 365 Sales Professional and Enterprise licenses, (ii) Dynamics 365 Customer Service Professional and Enterprise licenses, or (iii) Dynamics 365 Business Central and Dynamics 365 Finance or Supply Chain Management licenses if,

- Each Online Service is deployed under a separate instance, and
- Licensed users only access instances for which they are entitled.

Mixed deployments of Dynamics 365 Business Central services
Customers may not mix Dynamics 365 Business Central Premium and Dynamics 365 Business Central Essentials licenses on the same tenant.

Dynamics 365 Marketing
Promotional Laws, Regulations, and Industry Standards
Microsoft bears no responsibility for Customer's compliance with any applicable law, regulation, or industry standard governing the Customer's transmittal of promotional communications.

Dynamics Supply Chain Management, Finance, and Commerce Source Code
Customer may modify for its internal use the application source code for Dynamics 365 Supply Chain Management, Dynamics 365 Finance, and Dynamics 365 for Commerce.

Server Use Rights for Dynamics 365 User SLs, From SA User SLs and Add-on User SLs
The server use rights provisions below do not apply to Customers licensed for Dynamics 365 Sales Professional, Dynamics 365 Customer Service Professional, Dynamics 365 Marketing, Dynamics 365 Human Resources, or Customers licensed for Dynamics 365 online services through Open License, Open Value and Open Value Subscription.

Dynamics 365 for Operations on-premises Server
Customer's with active subscriptions for Dynamics 365 Supply Chain Management, Dynamics 365 Finance, or Dynamics 365 Commerce may,
- install any number of copies of the Dynamics 365 for Operations Server software on a network server or shared servers;
- install and use Dynamics AX 2012 R3 Server software in lieu of Dynamics 365 for Operations Server;
- allow access to the server software only to users and devices assigned a qualifying SL;
- receive and use updates related to government tax and regulatory requirements on the server software; and
- modify or create derivative works of plug-ins, runtime, and other components identified in printed or online documentation and use those derivative works, but only with the server software and only for Customer's internal purposes.

Dynamics 365 on-premises Server
Customers with active subscriptions for Dynamics 365 Sales Enterprise, Dynamics 365 Customer Service Enterprise, or Dynamics 365 Field Service may,
- install any number of copies of Dynamics 365 server (on-premises) software on a network server or shared servers;
- install Dynamics CRM 2016 Server software in lieu of Dynamics 365 On-Premise Server;
- allow access to the server software only to users and devices assigned a qualifying SL; and
- allow users and devices assigned one of the following CALs to access the version of the server software that is current as of the subscription start date: Dynamics 365 On-premises for Sales, Customer Service or Team Members CALs; or Dynamics CRM CAL. Users and devices assigned CALs with active Software Assurance may access new versions of the server software.

Dynamics 365 Business Central on-premises
Customers with active subscriptions for Dynamics 365 Business Central may,
- install any number of copies of Dynamics 365 Business Central on-premises software on a network server or shared servers;
- allow access to the server software only to users and devices assigned a qualifying SL; and
- allow users and devices assigned one of the following CALs to access the version of the server software that is current as of the subscription start date: Dynamics 365 Business Central Premium, Essentials, or Team Member CALs. Users and devices assigned CALs with an active maintenance plan may access new versions of the server software.

Microsoft Relationship Sales solution
Microsoft Relationship Sales solution includes Dynamics 365 Sales Enterprise and LinkedIn Sales Navigator Team or Enterprise. LinkedIn Sales Navigator Team/Enterprise is for the sole use of the Microsoft Relationship Sales solution Licensed User for the duration of the subscription.

LinkedIn Sales Navigator
LinkedIn Sales Navigator is provided by LinkedIn Corporation. Customer may use the LinkedIn Sales Navigator Service only to generate sales leads and not to recruit. Each user of LinkedIn Sales Navigator must be a member of LinkedIn and agree to be bound by the LinkedIn User Agreement available at https://www.linkedin.com/legal/preview/user-agreement. Despite anything to the contrary in Customer's volume licensing agreement (including these Online Services Terms or the DPA), the LinkedIn Privacy Policy available at https://www.linkedin.com/legal/privacy-policy will apply to Customer's use of the LinkedIn Sales Navigator service. LinkedIn Corporation (as data processor) and Customer (as data controller) will comply with the terms of the Data Processing Agreement located at https://legal.linkedin.com/dpa.

Dynamics 365 Operations Order Lines
Users or devices do not require an SL to indirectly (not through a client UI) execute the transaction types designated in the Dynamics 365 Licensing Guide (https://go.microsoft.com/fwlink/?LinkId=866544&clcid=0x409). The number of allowed transactions is limited to the number of order lines licensed.

Dynamics 365 Customer Insights
Microsoft Provided Data and Insights
Dynamics 365 Customer Insights may include Microsoft provided data and insights (including, but not limited to, market segment and brand affinity data and insights), which Customer may use for internal business purposes only.

Dynamics 365 Fraud Protection
Dynamics 365 Fraud Protection (DFP) processes Customer Data of DFP Customers as described in the Microsoft Dynamics 365 Trust Center to provide the service, which includes providing insights to Customer about the likelihood of fraud for the Customer's payment transactions and other fraud-related events ("Fraud Insights"). Customer acknowledges and agrees that (i) the Customer Data provided to the Online Service will be deidentified and combined with deidentified Customer Data of other D365 Fraud Protection Customers; (ii) Customer will be unable to access, extract, or delete the deidentified Customer Data that is used to generate Fraud Insights; and (iii) when Customer's subscription to Dynamics 365 Fraud Protection ends, Microsoft will continue to process the deidentified Customer Data for the sole purpose of providing Fraud Insights to other Dynamics 365 Fraud Protection Customers. Fraud Insights generated by Microsoft do not reveal Customer Data or other identifiable information of any Customer using Dynamics 365 Fraud Protection.

Restrictions on Use
Customer may only use the Fraud Insights to prevent fraud and help identify legitimate transactions. Customer agrees it will not use Fraud Insights (i) as the sole factor in determining whether to proceed with a payment transaction; (ii) as a factor in determining any person's financial status, financial history, creditworthiness, or eligibility for insurance, housing, or employment; or (iii) to make decisions that produce legal effects or significant personal outcomes concerning a person. Microsoft, in providing Dynamics 365 Fraud Protection, is not a "credit reporting agency" and does not provide "consumer reports" or "credit referencing" (as those practices are defined in the United States' Fair Credit Reporting Act, the United Kingdom's Financial Services and Markets Act, or similar laws).

Customer agrees to comply with any additional restrictions on the use of the Fraud Insights, as Microsoft may deem necessary. Customer shall confirm its compliance with the restriction on use of the Fraud Insights to Microsoft in writing within ten (10) days of receiving a request to do so by Microsoft. If Microsoft needs additional information to assure compliance with these restrictions, Customer will cooperate with Microsoft to provide such information, including documentation, within 30 business days of request.

Table of Contents / General Terms

Office 365 Services

Notices
The Bing Maps Notices in Attachment 1 apply. Any onboarding, migration, or deployment services provided to Customer are subject to the Professional Services Notice in Attachment 1.

Core Features for Office 365 Services
During the term of Customer's subscription, the Office 365 Services will substantially conform to the Core Features description provided (if any) in the Office 365 service-specific sections below, subject to Product restrictions or external factors (such as the recipient, message rate, message size and mailbox size limits for e-mail; default or Customer-imposed data retention policies; search limits; storage limits; Customer or end user configurations; and meeting capacity limits). Microsoft may permanently eliminate a functionality specified below only if it provides Customer a reasonable alternative functionality.

Administration Portal
Customer will be able to add and remove end users and domains, manage licenses, and create groups through the Microsoft Online Services Portal or its successor site.

Service Encryption with Customer Key
Customer assumes all risks of data deletion, inaccessibility, and service outages that result from any unavailability of an encryption key caused by Customer.

The Cortana core platform service integrated within Office 365 Services, in certain instances, may allow for users to connect to Microsoft services outside the Office 365 Services; if permitted by Customer, users electing to use such services are subject to terms of use other than these Online Services Terms for use of such services and with respect to which Microsoft is a data controller, as identified in product documentation.

Trials: Microsoft Teams Trial may only be initiated by individual end users. Customer may not initiate a Microsoft Teams Trial on behalf of end user employees.

Microsoft Threat Experts

Any services provided to Customer through the Microsoft Threat Experts Experts on Demand feature are subject to the Professional Services Notice in Attachment 1.

Yammer

For Office 365 Services that include Yammer, External Users invited to Yammer via external network functionality do not need User SLs.

Table of Contents / General Terms

Audio Services

Skype for Business Online (Plan 2)	Communication Credits
Audio Conferencing	Meeting Room
Calling Plan	Phone System
Common Area Phone	

Core Features for Office 365 Services

Skype for Business Online Plan 2 or their successor services will have the following Core Features capabilities:

Instant Messaging

An end user will be able to transfer a text message to another end user in real time over an Internet Protocol network.

Presence

An end user will be able to set and display the end user's availability and view another end user's availability.

Online Meetings

An end user will be able to conduct an Internet-based meeting that has audio and video conferencing functionality with other end users.

Notices

The H.264/MPEG-4 AVC and/or VC-1 Notices in Attachment 1 apply.

External Users and users not authenticated by Skype for Business Online

User SLs are not required for External Users and users not authenticated by the Skype for Business Online service.

Common Area Communications Device

A Common Area Communication Device ("CACD") is a device shared by multiple users who do not log into the device with their Office 365 credentials and which supports calls, meetings and/or conferencing over voice, Voice over IP, and/or video. Microsoft's Common Area Phone and Meeting Room offerings are Device SLs that may only be assigned to a CACD. Each CACD Licensed Device may be accessed and used by any number of users.

Calling Plan and Audio Conferencing Services (Calling/Conferencing Services)

Calling and Conferencing services are provided by the Microsoft Affiliate or other service provider authorized to administer them. Pricing for Calling and Conferencing services may include applicable taxes and fees. Calling and Conferencing services terms may vary from country to country. All included taxes, fees and country-specific terms of use are disclosed in the terms of use available on the Volume Licensing site at http://go.microsoft.com/fwlink/?LinkId=690247.

Exceeding the usage limitations for the applicable Calling and Conferencing service subscription plan as described in the terms of use may result in suspension of the services. Microsoft will provide reasonable notice before suspending Calling or Conferencing services, and customer will be able to make emergency calls during any period of suspension.

Important Information About Emergency Services

Customer must notify each user of a Calling Plan that Emergency Services operate differently than on traditional telephone services in the following ways: (i) Office 365 may not know the actual location of an Emergency Services caller, which could result in the call being routed to the wrong Emergency Services call center and/or emergency services being dispatched to the wrong location; (ii) if the user's device has no power, is experiencing a power outage or, for any reason, cannot otherwise access the Internet, the user cannot make an Emergency Services call through a Calling Plan service; and (iii) although Calling Plan services can be used anywhere in the world where an Internet connection is available, users

should not make an Emergency Services call from a location outside their home country because the call likely will not be routed to the appropriate call center in that location.

Table of Contents / General Terms

Exchange Online

Exchange Online (Plan 1 and 2)	Exchange Online Archiving for Exchange Server
Exchange Online K1	Data Loss Prevention
Exchange Online Archiving for Exchange Online	Office 365 Advanced Threat Protection

Core Features for Office 365 Services – Exchange Online

Exchange Online or its successor service will have the following Core Features capabilities:

Emails

An end user will be able to send email messages, receive email messages that originate from within and outside of Customer's organization, and access the end user's mailbox.

Mobile and Web Browser Access

Through the Microsoft Exchange ActiveSync protocol or a successor protocol or technology, Exchange Online will enable an end user to send and receive emails and update and view calendars from a mobile device that adequately supports such a protocol or technology. An end user will be able to send email messages, receive email messages that originate from within and outside of Customer's organization, and access the end user's mailbox, all from within a compatible web browser.

Retention Policies

Customer will be able to establish archive and deletion policies for email messages.

Deleted Item and Mailbox Recovery

Customer will be able to recover the contents of a deleted mailbox and an end user will be able to recover an item that has been deleted from one of the end user's email folders.

Multi-Mailbox Search

Customer will be able to search for content across multiple mailboxes within its organization.

Calendar

An end user will be able to view a calendar and schedule appointments, meetings, and automatic replies to incoming email messages.

Contacts

Through an Exchange Online-provided user interface, Customer will be able to create and manage distribution groups and an organization-wide directory of mail-enabled end users, distribution groups, and external contacts.

Core Features for Office 365 Services – Exchange Online Archiving

Exchange Online Archiving or its successor service will have the following Core Features capabilities:

Storage

Customer will be able to allow an end user to store email messages.

Retention Policies

Customer will be able to establish archive and deletion policies for email messages distinct from policies that an end user can apply to the end user's own mailbox.

Deleted Item and Mailbox Recovery

Customer, through Office 365 support services, will be able to recover a deleted archive mailbox, and an end user will be able to recover an item that has been deleted from one of the end user's email folders in the end user's archive.

Multi-Mailbox Search

Customer will be able to search for content across multiple mailboxes within its organization.

Legal Hold

Customer will be able to place a "legal hold" on an end user's primary mailbox and archive mailbox to preserve the content of those mailboxes.

Archiving
Archiving may be used for messaging storage only with Exchange Online Plans 1 and 2.

Archiving for Exchange Server
Users licensed for Exchange Server 2013 Standard Client Access License may access the Exchange Server 2013 Enterprise Client Access License features necessary to support use of Exchange Online Archiving for Exchange Server.

Smartphone and Tablet Devices
Each user to whom Customer assigns an Exchange Online User SL may (i) use Microsoft Outlook for mobile devices for commercial purposes and (ii) sign in to Microsoft Outlook with their org ID on up to five smartphones and five tablets.

Exchange Online Plan 2 from Exchange Hosted Archive Migration
Exchange Online Plan 2 is a successor Online Service to Exchange Hosted Archive. If Customer renews from Exchange Hosted Archive into Exchange Online Plan 2 and has not yet migrated to Exchange Online Plan 2, Customer's licensed users may continue to use the Exchange Hosted Archive service subject to the terms of the March 2011 Product Use Rights until the earlier of Customer's migration to Exchange Online Plan 2 or the expiration of Customer's Exchange Online Plan 2 User SLs. The Product Use Rights is located at http://go.microsoft.com/?linkid=9839206.

Office 365 Data Loss Prevention Device License
If Customer is licensed for Office 365 Data Loss Prevention by Device, all users of the Licensed Device are licensed for the Online Service.

Service Level Agreement
There is no SLA for Office 365 Advanced Threat Protection.

Table of Contents / General Terms

Microsoft Stream

Notices
The H.264/AVC Visual Standard, VC-1 Video Standard, MPEG-4 Part 2 Visual Standard, and MPEG-2 Video Standard Notices in Attachment 1 apply.

Stream Live Events
Stream Live Events are subject to the following:

a. Stream Live Events may not be greater than four (4) hours in length;
b. Stream Live Events attendees may not exceed 10,000; and
c. Stream Live Events are limited to fifteen (15) per customer at any single point in time.

Table of Contents / General Terms

Microsoft Teams

Notices
The H.264/MPEG-4 AVC Notice in Attachment 1 applies to all Office 365 Services that include Microsoft Teams.

Health Sector Customers
Customer is solely responsible for: (1) the accuracy and adequacy of information and Data furnished through use of Microsoft Teams; (2) implementing a secure application-to-application authentication method between any Customer application and/or service and Microsoft Teams; (3) obtaining appropriate consent from end users in connection with end user's and Customer's use of Microsoft Teams; and (4) displaying appropriate warnings, disclaimers, and acknowledgements to end users in connection with end user's and Customers use of Microsoft Teams.

CUSTOMER ACKNOWLEDGES THAT THE ONLINE SERVICES (MICROSOFT TEAMS SERVICE AND APPLICATIONS) (1) ARE NOT INTENDED OR MADE AVAILABLE AS A MEDICAL DEVICE (OR MEDICAL DEVICES) FOR THE DIAGNOSIS OF DISEASE OR OTHER CONDITIONS, OR IN THE CURE, MITIGATION, TREATMENT OR PREVENTION OF DISEASE, OR OTHERWISE TO BE USED AS A COMPONENT OF ANY CLINICAL OFFERING OR PRODUCT, AND NO LICENSE OR RIGHT IS GRANTED TO USE THE ONLINE SERVICES FOR SUCH PURPOSES, (2) IS NOT DESIGNED OR INTENDED TO BE A SUBSTITUTE FOR PROFESSIONAL MEDICAL ADVICE, DIAGNOSIS, TREATMENT, OR JUDGMENT AND SHOULD NOT BE USED TO REPLACE OR AS A SUBSTITUTE FOR PROFESSIONAL MEDICAL ADVICE, DIAGNOSIS, TREATMENT, OR JUDGMENT, AND (3) SHOULD NOT BE USED FOR MEDICAL EMERGENCIES. CUSTOMER IS SOLELY RESPONSIBLE FOR ANY PERSONAL INJURY OR DEATH THAT MAY OCCUR AS A RESULT OF ITS USE OF MICROSOFT TEAMS AND APPLICATIONS, INCLUDING (WITHOUT LIMJITATION) ANY SUCH INJURIES TO END USERS OR CUSTOMER PATIENTS.

Trials
Microsoft Teams Exploratory Experience may only be initiated by individual end users. Customer may not initiate a Microsoft Teams Exploratory Experience on behalf of end user employees.

Table of Contents / General Terms

Office 365 Applications

Office 365 Business
Office 365 ProPlus
Visio Online (Plan 1 and 2)

Service Level Agreement
There is no SLA for Visio Online.

Installation and Use Rights
Each user to whom Customer assigns a User SL must have a work or school account in order to use the software provided with the subscription. These users:

- may activate the software provided with the SL on up to five concurrent OSEs for local or remote use;
- may also install and use the software, with shared computer activation, on a shared device, a Network Server, or on Microsoft Azure or with a Qualified Multitenant Hosting Partner ("QMTH"). Rights to install and use the software with a QMTH do not apply if the QMTH is using a Listed Provider as a Data Center Provider, as those terms are defined in the Product Terms. The Product Terms is located at http://go.microsoft.com/?linkid=9839207. A list of Qualified Multitenant Hosting Partners and additional deployment requirements are available at www.office.com/sca. This shared computer activation provision only applies to Customers licensed for Office 365 Business when Office 365 Business is licensed as a component of Microsoft 365 Business;
- must connect each device upon which user has installed the software to the Internet at least once every 30 days or the functionality of the software may be affected; and
- may use Internet-connected Online Services provided as part of ProPlus [and governed by this OST]. Additionally, if permitted by Customer, users may elect to use connected services subject to terms of use other than this OST and with respect to which Microsoft is a data controller, as identified in product documentation.
  - The Online Services will permit Customer to enable or disable these optional connected services; and
  - Customer is responsible for evaluating, enabling or disabling the availability of optional connected services to its users.

Smartphone and Tablet Devices
Each user to whom Customer assigns an Office 365 Business or Office 365 ProPlus User SL may (i) use Microsoft Office for mobile devices for commercial purposes and (ii) sign in to Microsoft Office with their org ID on up to five smartphones and five tablets.

The following terms apply only to Office 365 ProPlus

Office Home & Student 2013 RT Commercial Use
The commercial use restriction for Office Home & Student 2013 RT is waived for each Office 365 ProPlus User SL. Except as provided in this section, the terms provided with the Office Home & Student 2013 RT License will govern.

Office Online Server
For each Office 365 ProPlus subscription, Customer may install any number of copies of Office Online Server on any Server dedicated to Customer's use. Any dedicated server that is under the management or control of an entity other than Customer or one of its Affiliates is subject to the Outsourcing Software Management clause of the Product Terms. Each Office 365 ProPlus user may use the Office Online Server software. This provision does not apply to Customers that license this Product under the Microsoft Online Subscription Agreement, Microsoft Cloud Agreement, Microsoft Customer Agreement, or other Microsoft agreement that cover Online Services only.

Table of Contents / General Terms

Office for the web

Core Features for Office 365 Services
Office for the web or its successor service will have the following Core Features capabilities:
An end user will be able to create, view, and edit documents in Microsoft Word, Excel, PowerPoint, and OneNote file types that are supported by Office for the web or its successor service.

External Users
External Users invited to site collections via Share-by-Mail functionality do not need User SLs with Office for the web.

Table of Contents / General Terms

OneDrive for Business

External Users
External Users invited to site collections via Share-by-Mail functionality do not need User SLs with OneDrive for Business.

Table of Contents / General Terms

Project

Project Online Essentials
Project Plan 1
Project Plan 3
Project Plan 5

Installation and Use Rights for Project application
Each user to whom Customer assigns a Project Plan 3 or Plan 5 User SL must have a Microsoft Account in order to use the software provided with the subscription. These users:

- may activate the software provided with the SL on up to five concurrent OSEs for local or remote use;
- may also install and use the software, with shared computer activation, on a shared device, a Network Server, or on Microsoft Azure or with a Qualified Multitenant Hosting Partner ("QMTH"). Rights to install and use the software with a QMTH do not apply if the QMTH is using a Listed Provider as a Data Center Provider, as those terms are defined in the Product Terms. The Product Terms is located at http://go.microsoft.com/?linkid=9839207. A list of Qualified Multitenant Hosting Partners and additional deployment requirements is available at www.office.com/sca; and
- must connect each device upon which user has installed the software to the Internet at least once every 30 days or the functionality of the software may be affected.

Use of SharePoint Online
Rights to the SharePoint Online functionality provided with a Project Plan 3 or Plan 5 SL are limited to storing and accessing data in support of Project online.

Table of Contents / General Terms

SharePoint Online

SharePoint Online (Plan 1 and 2)
SharePoint Online K1
Duet Enterprise Online for Microsoft SharePoint and SAP

Core Features for Office 365 Services
SharePoint Online or its successor service will have the following Core Features capabilities:

Collaboration Sites
An end user will be able to create a web browser-accessible site through which the end user can upload and share content and manage who has permission to access that site.

Storage
Customer will be able to set storage capacity limits for a site created by an end user.

External Users
External Users invited to site collections via Share-by-Mail functionality do not need User SLs with SharePoint Online K1, Plan 1 and Plan 2.

Storage Add-on SLs
Office 365 Extra File Storage is required for each gigabyte of storage in excess of the storage provided with User SLs for SharePoint Online Plans 1 and 2.

Table of Contents / General Terms

Other Online Services

Bing Maps Mobile Asset Management Platform

Service SLs
A Service SL is required to access the services via the Bing Maps Mobile Asset Management Platform. A Service SL must be purchased with at least one of the following qualifying Add-on SLs for each asset:

- Mobile Asset Management for North America Add-on SL (routing or without routing)
- Mobile Asset Management for Europe Add-on SL (routing or without routing), or
- Mobile Asset Management for Rest of World Add-on SL (routing or without routing)

Bing Maps APIs
A Customer with a license to use the Bing Maps Mobile Asset Management Platform Bing Maps APIs in accordance with the Microsoft Bing Maps Platform API Terms of Use and Bing Maps Documentation, including any successors thereto, located at https://aka.ms/bingmapsplatformapistou and https://aka.ms/bingmapsplatformsdks/.

Bing Maps Privacy
The Microsoft Privacy Statement (located at: https://go.microsoft.com/fwlink/?LinkId=521839) and privacy terms in the Microsoft Bing Maps Platform API Terms of Use apply to Customer's use of the Bing Maps Mobile Asset Management Platform.

Table of Contents / General Terms

Bing Maps Transactions and Users

Bing Maps Transactions	Bing Maps Light Known User
Bing Maps Known User	

Authenticated Users
Users that are authenticated by Customer's programs that access the service through the Bing Maps APIs must have a SL.

Bing Maps APIs
A Customer with a license to use Bing Maps Transactions and Users may use Bing Maps APIs in accordance with the Microsoft Bing Maps Platform API Terms of Use and Bing Maps Documentation, including any successors thereto, located at https://aka.ms/bingmapsplatformapistou and https://aka.ms/bingmapsplatformsdks/.

Bing Maps Privacy
The Microsoft Privacy Statement (located at https://go.microsoft.com/fwlink/?LinkId=521839) and privacy terms in the Microsoft Bing Maps Platform API Terms of Use apply to Customer's use of Bing Maps.

Table of Contents / General Terms

Microsoft Power Platform

Microsoft Power Automate	Microsoft Power BI Pro
Microsoft Power Apps	Microsoft Power BI Premium

Notices
The Bing Maps, H.264/AVC Visual Standard, VC-1 Video Standard, MPEG-4 Part 2 Visual Standard, and MPEG-2 Video Standard Notices in Attachment 1 apply.

Microsoft Power BI

Definitions
"Customer Application" means an application or any set of applications that adds primary and significant functionality to the Embedded Capabilities and that is not primarily a substitute for any portion of Microsoft Power BI services.
"Embedded Capabilities" means the Power BI APIs and embedded views for use by an application.

Hosting Exception for Embedded Capabilities
Customer may create and maintain a Customer Application and, despite anything to the contrary in Customer's volume licensing agreement, combine Embedded Capabilities with Customer Data owned or licensed by Customer or a third party, to create a Customer Application using the

Embedded Capabilities and the Customer Data together. Any Power BI content accessed by the Customer Application or its end users must be stored in Microsoft Power BI Premium capacity. Customer may permit third parties to access and use the Embedded Capabilities in connection with the use of that Customer Application. Customer is responsible for that use and for ensuring that these terms and the terms and conditions of Customer's volume licensing agreement are met by that use.

Limitations

Customer may not

- resell or redistribute the Microsoft Power BI services, or
- allow multiple users to directly or indirectly access any Microsoft Power BI feature that is made available on a per user basis.

Access without a User SL

A User SL is not required to view content in Power BI Premium capacity that is shared through the embed APIs or embedded views functionality. With Power BI Premium P series only, a User SL is also not required to view content in Power BI Premium capacity that is shared through the apps or email subscription features, or through Power BI Report Server.

Publish to Web

Customer may use the publish to web functionality to share content only on a publicly available website. Customer may not use this functionality to share content internally. Microsoft may display content published through the publish to web functionality on a public website or gallery.

Microsoft Power Apps

Restricted Entities

Customer may not create, modify, or delete any data from entities of the type designated as "restricted" in product documentation at https://go.microsoft.com/fwlink/?linkid=868812. Customer has read-only access to such restricted entities.

Unauthenticated External Users

External Users not authenticated by Power Apps do not need a User SL to access Power Portals.

Table of Contents / General Terms

Microsoft 365 - Unattended License

Service Level Agreement

There is no SLA for Microsoft 365 - Unattended License

Definitions

"Robotic Process Automation", otherwise known as "RPA" or "bots" means an application, or any set of applications used to capture data and manipulate applications to perform repetitive tasks. Bots operate upon any UI element of Windows 10 within an OSE and/or operates upon any Office application in any OSE.

"Unattended Bot" – Any bot that doesn't strictly conform to the definition of "Attended Bot" shall be considered an "Unattended Bot."

"Attended Bot" - An Attended Bot assists a person to execute automation on the person's local and/or remote workstations. It operates concurrently with the person on the same workstation/s to accomplish repetitive tasks and is triggered by explicit actions of that person.

Assignment and Use Rights

- Customer may assign a Microsoft 365 A3/E3 - Unattended License to an Unattended bot running on hardware dedicated to Customer's use.
- Each Microsoft 365 A3/E3 - Unattended License allows the use of the M365 A3/E3 suite in only a single physical or virtual OSE for Robotic Process Automation.
- License reassignment for bots follow the same rules for users and devices as if the bot is a user. (See License Reassignment)

Use Limitation

- Unattended bots may not create or replicate activities or workflows on behalf of an unlicensed user or device. (See Multiplexing)
- Microsoft reserves the right to restrict or disable Microsoft API calls with reasonable notice, due to unreasonable amount of bandwidth, adversely impacting the stability of Microsoft API's, or adversely affecting the behavior of other apps.

Table of Contents / General Terms

GitHub Offerings

GitHub Enterprise
GitHub Actions
GitHub Insights
GitHub Learning Lab for Organizations
GitHub One
GitHub Advanced Security
GitHub Packages

GitHub Offerings are provided by GitHub, Inc. By using GitHub Offerings, Customer agrees to be bound by the GitHub terms available at https://aka.ms/github_terms. Notwithstanding anything to the contrary in Customer's volume licensing agreement (including these Online Services Terms and the DPA), the GitHub Privacy Statement available at https://help.github.com/articles/github-privacy-statement/ and the GitHub Data Protection Addendum located at https://aka.ms/github_terms will apply to Customer's use of GitHub Offerings, including GitHub Enterprise licensed standalone or as Visual Studio Enterprise or Professional with GitHub Enterprise.

GitHub Actions and GitHub Packages
Customer's Licensed Users of GitHub Enterprise or an offering that includes GitHub Enterprise may access and use GitHub Actions and GitHub Packages licensed by Customer.

GitHub Advanced Security and GitHub Insights
Customer's Licensed Users of GitHub Enterprise or an offering that includes GitHub Enterprise may access and use Git Hub Advanced Security and GitHub Insights, provided that all such users are also assigned GitHub Advanced Security and GitHub Insights User SLs.

GitHub One - Premium Support for GitHub Enterprise
GitHub One includes an enhanced level of technical support provided by GitHub, Inc. The GitHub Engineering Direct offer requires a customer to have Microsoft Premier or Unified Support as a pre-requisite. By using GitHub technical support, Customer agrees to be bound by the GitHub terms available at https://aka.ms/githubsupport.

Table of Contents / General Terms

Microsoft Cloud App Security

External User Allowance
In addition to access by its Licensed Users, Customer may permit External Users to access the service in connection with access to Customer's resources using SharePoint Online, OneDrive, Teams and other Microsoft hosted services.

Notices
The Bing Maps and Professional Services notices in Attachment 1 apply.

Table of Contents / General Terms

Microsoft Graph data connect for ISVs

Service SLs
Customer must have an SL for each user data Customer's application processes. For purposes of Microsoft Graph data connect for ISVs (Independent Software Vendors), "user data" is data sourced from the user's Office 365 account, which is held by the Customer's customer. Access to user data is provided to Customer by the Customer's customer.

Service Level Agreement
There is no SLA for Microsoft Graph data connect for ISVs.

Table of Contents / General Terms

Microsoft Healthcare Bot Service

Definitions
"Customer Healthcare Bot Application" means an application or any set of applications that adds primary and significant functionality to the Microsoft Healthcare Bot Service and that is not primarily a substitute for the Microsoft Healthcare Bot Service.

Customer Obligations
Customer is solely responsible for: (1) the accuracy and adequacy of information and Data furnished through use of the Microsoft Healthcare Bot Service; (2) implementing a secure application-to-application authentication method between the Customer Healthcare Bot Application and the Microsoft Healthcare Bot Service; (3) obtaining appropriate consent from end users in connection with their use of the Customer Healthcare Bot

Application; and (4) displaying appropriate warnings, disclaimers, and acknowledgements to end users in connection with their use of the Customer Healthcare Bot Application, including, as applicable, those set forth in the following form.

Use Limitation

CUSTOMER ACKNOWLEDGES THAT THE MICROSOFT HEALTHCARE BOT SERVICE (1) IS NOT INTENDED OR MADE AVAILABLE AS A MEDICAL DEVICE (OR MEDICAL DEVICES) FOR THE DIAGNOSIS OF DISEASE OR OTHER CONDITIONS, OR IN THE CURE, MITIGATION, TREATMENT OR PREVENTION OF DISEASE, OR OTHERWISE TO BE USED AS A COMPONENT OF ANY CLINICAL OFFERING OR PRODUCT, AND NO LICENSE OR RIGHT IS GRANTED TO USE THE MICROSOFT HEALTHCARE BOT SERVICE FOR SUCH PURPOSES, (2) IS NOT DESIGNED OR INTENDED TO BE A SUBSTITUTE FOR PROFESSIONAL MEDICAL ADVICE, DIAGNOSIS, TREATMENT, OR JUDGMENT AND SHOULD NOT BE USED TO REPLACE OR AS A SUBSTITUTE FOR PROFESSIONAL MEDICAL ADVICE, DIAGNOSIS, TREATMENT, OR JUDGMENT, AND (3) SHOULD NOT BE USED FOR EMERGENCIES AND DOES NOT SUPPORT EMERGENCY CALLS. CUSTOMER ACKNOWLEDGES THAT THE CUSTOMER HEALTHCARE BOT APPLICATION WILL CONSTITUTE CUSTOMER'S OWN PRODUCT OR SERVICE, SEPARATE AND APART FROM THE MICROSOFT HEALTHCARE BOT SERVICE. CUSTOMER IS SOLELY RESPONSIBLE FOR THE DESIGN, DEVELOPMENT, AND IMPLEMENTATION OF THE CUSTOMER HEALTHCARE BOT APPLICATION, AND FOR PROVIDING END USERS WITH APPROPRIATE WARNINGS PERTAINING TO USE OF THE CUSTOMER HEALTHCARE BOT APPLICATION. CUSTOMER IS SOLELY RESPONSIBLE FOR ANY PERSONAL INJURY OR DEATH THAT MAY OCCUR AS A RESULT OF ITS USE OF THE MICROSOFT HEALTHCARE BOT SERVICE IN CONNECTION WITH THE CUSTOMER HEALTHCARE BOT APPLICATION, INCLUDING (WITHOUT LIMITATION) ANY SUCH INJURIES TO END USERS.

Table of Contents / General Terms

Microsoft Intune

Microsoft Intune (per user)	Microsoft Intune Add-on for System Center Configuration Manager and System Center Endpoint Protection (per user, per device) ("Microsoft Intune Add-On")
Microsoft Intune for Devices	
Microsoft Intune for EDU (per user, per device)	

Notices

Any deployment services provided to Customer are subject to the Professional Services Notice in Attachment 1.

Manage Devices and Applications

Each User to whom Customer assigns a User SL may access and use the Online Services and related software (including System Center software) to manage applications and up to fifteen devices. Management of a device accessed by more than one user requires a User SL for each user.

Microsoft Intune for Devices

Microsoft Intune for Devices may only be linked to devices that are not affiliated with specific users. Product features with user affinity, including but not limited to Conditional Access, App Protection, and optional app installation, cannot be used under Microsoft Intune for Devices SLs. Applications that are typically mapped to specific users, such as Outlook and OneDrive, may not be used under this service.

Storage Add-on SL

A Storage Add-on SL is required for each gigabyte of storage in excess of the storage provided with the base subscription.

Windows Software Components in System Center Software

The System Center software includes one or more of the following Windows Software Components: Microsoft .NET Framework, Micro soft Data Access Components, PowerShell software and certain .dlls related to Microsoft Build, Windows Identity Foundation, Windows Library for JavaScript, Debghelp.dll, and Web Deploy technologies. The license terms governing use of the Windows Software Components are in the Windows 8.1 Pro and Enterprise section of the Product Terms. The Product Terms is located at http://go.microsoft.com/?linkid=9839206.

SQL Server Technology and Benchmarking

The Software included with the Online Service includes SQL Server-branded components other than a SQL Server Database. Those components are licensed to Customer under the terms of their respective licenses, which can be found in the installation directory or unifie d installer of the software. Customer must obtain Microsoft's prior written approval to disclose to a third party the results of any benchmark t est of these components or the software that includes them.

Table of Contents / General Terms

Microsoft Learning

Microsoft Learning E-Reference Library

Any person that has valid access to Customer's computer or internal network may copy and use the documentation for Customer's internal reference purposes. Documentation does not include electronic books.

Microsoft Learning Imagine Academy Service SL
A Service SL is required for each Location that accesses or uses any Microsoft Imagine Academy service or benefit. Location is defined as a physical site with staff under the same administrator, such as a principal, in a single building or group of buildings located on the same campus.

Microsoft Learning Imagine Academy Program Guidelines
The Imagine Academy program guidelines, located at http://www.microsoft.com/itacademy, apply to Customer's use of the Microsoft Learning Imagine Academy and its benefits.

Microsoft Learning Imagine Academy Program Benefits Provided by Third-Party
Program benefits may only be used by a licensed institution's faculty, staff and students currently enrolled in the licensed institution.

Table of Contents / General Terms

Microsoft Search in Bing

Microsoft Search in Bing
"Microsoft Search in Bing" means the service that displays enterprise search results from internal resources (e.g. intranet, files, people information) to Customer users who are logged into the service via their work or school account.

Microsoft Search in Bing Privacy
When a user enters a search query in Microsoft Search in Bing, two simultaneous search requests occur: (1) a search of Customer's internal resources, for which the query and results returned are Customer Data for purposes of these Online Services Terms, and (2) a separate search of public results from Bing.com, for which the query and results returned are not Customer Data. These Online Services Terms and the DPA apply only to Microsoft Search in Bing. The Microsoft Privacy Statement located at https://go.microsoft.com/fwlink/?LinkId=521839 applies to public search on Bing.com.

Table of Contents / General Terms

Microsoft Threat Protection

Data Handling
Microsoft Threat Protection integrates Customer Data from multiple Online Services. Applicable Customer Data will be transferred from other Microsoft services into Microsoft Threat Protection and from Microsoft Threat Protection back to applicable Microsoft services. Microsoft's data-handling commitments applicable to Microsoft Threat Protection will apply to such Customer Data. Such commitments may differ from Microsoft's commitments for the services from which that Customer Data was transferred. Further, Customer Data will be stored at rest in the Geo in which Microsoft Threat Protection is provisioned, which may differ from the Geo in which other services are provisioned.

Table of Contents / General Terms

Minecraft: Education Edition

Notices
The Bing Maps Notices in Attachment 1 apply.

Table of Contents / General Terms

Office 365 Developer

No Production Use of Office 365 Developer
Each user to whom Customer assigns a User SL may use the Online Service to design, develop, and test Customer's applications to make them available for Customer's Office 365 Online Services, on-premises deployments or for the Microsoft Office Store. The Online Service is not licensed for production use.

Office 365 Developer End Users
Customer's end users do not need a SL to access Office 365 Developer to perform acceptance tests or provide feedback on Customer programs.

Table of Contents / General Terms

Microsoft Defender Advanced Threat Protection

Data Retention

Microsoft Defender Advanced Threat Protection does not contain extractable Customer Data therefore the Customer Data extraction terms in the DPA do not apply.

Table of Contents / General Terms

Attachment 1 – Notices

Online Services excluded from the DPA

The terms of the DPA do not apply to: Bing Maps Mobile Asset Management Platform, Bing Maps Transactions and Users, Bing Search Services, GitHub Enterprise, LinkedIn Sales Navigator, Azure Stack Hub, Microsoft Graph data connect for ISVs, Microsoft Genomics, and Visual Studio App Center Test. Each of these Online Services are governed by the privacy and security terms in the applicable Online Service-specific Terms.

Table of Contents / General Terms

Core Online Services

The term "Core Online Services" applies only to the services in the table below, excluding any Previews.

Online Services	
Microsoft Dynamics 365 Core Services	The following services, each as a standalone service or as included in a Dynamics 365 branded plan or application: Dynamics 365 Customer Service Enterprise, Dynamics 365 Customer Service Professional, Dynamics 365 Customer Service Insights, Dynamics 365 Field Service, Dynamics 365 Business Central, Dynamics 365 Supply Chain Management, Dynamics 365 Finance, Dynamics 365 Marketing, Dynamics 365 Project Service Automation, Dynamics 365 Commerce, Dynamics 365 Human Resources, Dynamics 365 Sales Enterprise, and Dynamics 365 Sales Professional. Dynamics 365 Core Services do not include (1) Dynamics 365 Services for supported devices or software, which includes but is not limited to Dynamics 365 for apps, tablets, phones, or any of these; (2) LinkedIn Sales Navigator; or (3) except as expressly defined in the licensing terms for the corresponding service, any other separately-branded service made available with or connected to Dynamics 365 Core Services.
Office 365 Services	The following services, each as a standalone service or as included in an Office 365-branded plan or suite: Compliance Manager, Customer Lockbox, Exchange Online Archiving, Exchange Online Protection, Exchange Online, Microsoft Bookings, Microsoft Forms, Microsoft MyAnalytics, Microsoft Planner, Microsoft StaffHub, Microsoft Stream, Microsoft Teams (including Bookings, Lists, and Shifts), Microsoft To-Do, Office 365 Advanced Threat Protection, Office 365 Video, Office for the web, OneDrive for Business, Project (except Roadmap and Project for the web), SharePoint Online, Skype for Business Online, Sway, Whiteboard, Yammer Enterprise and, for Kaizala Pro, Customer's organizational groups managed through the admin portal and chats between two members of Customer's organization. Office 365 Services do not include Office 365 ProPlus, any portion of PSTN Services that operate outside of Microsoft's control, any client software, or any separately branded service made available with an Office 365-branded plan or suite, such as a Bing or a service branded "for Office 365."
Microsoft Azure Core Services	API Management, App Service (API Apps, Logic Apps, Mobile Apps, Web Apps), Application Gateway, Application Insights, Automation, Azure Active Directory, Azure Cache for Redis, Azure Container Registry (ACR), Azure Container Service, Azure Cosmos DB (formerly DocumentDB), Azure Database for MySQL, Azure Database for PostgreSQL, Azure Databricks, Azure DevOps Services, Azure DevTest Labs, Azure DNS, Azure Information Protection (including Azure Rights Management), Azure Kubernetes Service, Azure NetApp Files, Azure Resource Manager, Azure Search, Backup, Batch, BizTalk Services, Cloud Services, Computer Vision, Content Moderator, Data Catalog, Data Factory, Data Lake Analytics, Data Lake Store, Event Hubs, Express Route, Face, Functions, HDInsight, Import/Export, IoT Hub, Key Vault, Load Balancer, Log Analytics (formerly Operational Insights), Azure Machine Learning Studio, Media Services, Microsoft Azure Portal, Multi-Factor Authentication, Notification Hubs, Power BI Embedded, QnA Maker, Scheduler, Security Center, Service Bus, Service Fabric, Site Recovery, SQL Data Warehouse, SQL Database, SQL Server Stretch Database, Storage, StorSimple, Stream Analytics, Text Analytics, Traffic Manager, Virtual Machines, Virtual Machine Scale Sets, Virtual Network, and VPN Gateway
Microsoft Cloud App Security	The cloud service portion of Microsoft Cloud App Security.
Microsoft Intune Online Services	The cloud service portion of Microsoft Intune such as the Microsoft Intune Add-on Product or a management service provided by Microsoft Intune such as Mobile Device Management for Office 365.
Microsoft Power Platform Core Services	The following services, each as a standalone service or as included in an Office 365 or Microsoft Dynamics 365 branded plan or suite: Microsoft Power BI, Microsoft Power Apps, and Microsoft Power Automate. Microsoft Power Platform Core Services do not include any client software, including but not limited to Power BI Report Server, the Power BI, PowerApps or Microsoft Power Automate mobile applications, Power BI Desktop, or Power Apps Studio.
Microsoft Defender Advanced Threat Protection Services	The following cloud service portions of Microsoft Defender Advanced Threat Protection: Attack Surface Reduction, Next Generation Protection, Endpoint Detection & Response, Auto Investigation & Remediation, Threat & Vulnerability Management, SmartScreen.

Security Practices and Policies for Core Online Services

In addition to the security practices and policies for Online Services in the DPA, each Core Online Service also complies with the control standards and frameworks shown in the table below and implements and maintains the security measures set forth in Appendix A of the DPA for the protection of Customer Data.

Online Service	SSAE 18 SOC 1 Type II	SSAE 18 SOC 2 Type II
Office 365 Services	Yes	Yes
Microsoft Dynamics 365 Core Services	Yes*	Yes*
Microsoft Azure Core Services	Varies**	Varies**
Microsoft Cloud App Security	Yes	Yes
Microsoft Intune Online Services	Yes	Yes
Microsoft Power Platform Core Services	Yes	Yes
Microsoft Defender Advanced Threat Protection Services	Yes	Yes

**Does not include Microsoft Dynamics 365 Marketing.*

***Current scope is detailed in the audit report and summarized in the Microsoft Trust Center.*

Location of Customer Data at Rest for Core Online Services

For the Core Online Services, Microsoft will store Customer Data at rest within certain major geographic areas (each, a Geo) as follows:

- **Office 365 Services.** If Customer provisions its tenant in Australia, Canada, the European Union, France, Germany, India, Japan, Norway, South Africa, South Korea, Switzerland, the United Kingdom, the United Arab Emirates, or the United States, Microsoft will store the following Customer Data at rest only within that Geo: (1) Exchange Online mailbox content (e-mail body, calendar entries, and the content of e-mail attachments), (2) SharePoint Online site content and the files stored within that site, and (3) files uploaded to OneDrive for Business.
- **Microsoft Intune Online Services**. When Customer provisions a Microsoft Intune tenant account to be deployed within an available Geo, then, for that service, Microsoft will store Customer Data at rest within that specified Geo except as noted in the Microsoft Intune Trust Center.
- **Microsoft Power Platform Core Services**. If Customer provisions its tenant in Australia, Canada, Asia Pacific, France, India, Japan, the European Union, United Kingdom, or the United States, Microsoft will store Customer Data at rest only within that Geo, except as noted in the data location section of the Microsoft Power Platform Trust Center.
- **Microsoft Azure Core Services**. If Customer configures a particular service to be deployed within a Geo then, for that service, Microsoft will store Customer Data at rest within the specified Geo. Certain services may not enable Customer to configure deployment in a particular Geo or outside the United States and may store backups in other locations. Refer to the Microsoft Trust Center (which Microsoft may update from time to time, but Microsoft will not add exceptions for existing Services in general release) for more details.
- **Microsoft Cloud App Security**. If Customer provisions its tenant in the European Union or the United States, Microsoft will store Customer Data at rest only within that Geo, except as described in the Microsoft Cloud App Security Trust Center.
- **Microsoft Dynamics 365 Core Services**. When Customer provisions a Dynamics 365 Core Service to be deployed within an available Geo, then, for that service, Microsoft will store Customer Data at rest within that specified Geo, except as described in the Microsoft Dynamics 365 Trust Center.
- **Microsoft Defender Advanced Threat Protection Services**. When Customer provisions a Microsoft Defender Advanced Threat Protection tenant to be deployed within an available Geo, then, for that service, Microsoft will store Customer Data at rest within that specified Geo except as noted in the Microsoft Defender Advanced Threat Protection Trust Center.

Table of Contents / General Terms

Bing Maps

The Online Service or its included software includes use of Bing Maps. Any content provided through Bing Maps, including geocodes, can only be used within the product through which the content is provided. Customer's use of Bing Maps is governed by the Bing Maps End User Terms of Use available at go.microsoft.com/?linkid=9710837 and the Microsoft Privacy Statement available at go.microsoft.com/fwlink/?LinkID=248686.

Table of Contents / General Terms

Professional Services

Professional Services are provided subject to the "Professional Services Terms" below. If, however, Professional Services are provided pursuant to a separate agreement, then the terms of that separate agreement will apply to those Professional Services. Data protection and security terms for Professional Services Data are in the DPA.

The Professional Services to which this Notice applies are not Online Services, and the rest of the Online Services Terms do not apply unless expressly made applicable by the Professional Services Terms below.

Professional Services Terms

Obligations of the Parties; Warranties

Microsoft warrants that all Professional Services will be performed with professional care and skill. If Microsoft fails to do so and Customer notifies Microsoft within 90 days of the date of performance, then Microsoft will either re-perform the Professional Services or return the price paid for them as Customer's sole remedy for breach of the Professional Services warranty. Notwithstanding the foregoing, **Services Deliverables that are provided without charge are provided "AS-IS," WITHOUT ANY WARRANTY. Microsoft provides no 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**.

Customer will perform its applicable responsibilities and obligations to support Microsoft's performance of the Professional Services, as specified in the description of each Professional Service. Customer may not use Professional Services or Services Deliverables in any way prohibited by the Acceptable Use Policy and must comply with all laws and regulations applicable to its use of Professional Services and Services Deliverables, including laws related to privacy, Personal Data, biometric data, data protection and confidentiality of communications. Customer is solely responsible for testing, deploying, maintaining and supporting Services Deliverables that are provided or recommended without charge by Microsoft.

Limitation of Liability

To the extent permitted by applicable law, each party's total liability for all claims relating to Professional Services will be limited to the amounts Customer was required to pay for the Professional Services or the limitation of liability for the Online Service with which the Professional Services are offered, whichever is greater. For Professional Services and Services Deliverables provided free of charge and Services Deliverables 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. **In no event will either party be liable for indirect, incidental, special, punitive, or consequential damages, including loss of use, loss of profits, or interruption of business, however caused or on any theory of liability in relation to the Professional Services, or Services Deliverables. No limitation or exclusions will apply to liability arising out of either party's (1) confidentiality obligations (except for all liability limited to Customer Data and Professional Services Data, which remain subject to the limitations and exclusions above); or (2) violation of the other party's intellectual property rights.**

Fixes

"Fixes" are Product fixes, modifications or enhancements, or their derivatives, that Microsoft either releases generally (such as service packs) or that Microsoft provides to Customer to address a specific issue. 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 terms Microsoft provides with the Fix will apply.

Pre-Existing Work

"Pre-Existing Work" means any computer code or non-code based written materials developed or otherwise obtained independent of Customer's volume licensing agreement. All rights in Pre-Existing Work shall remain the sole property of the party providing the Pre-Existing Work. Each party may use, reproduce and modify the other party's Pre-Existing Work only as needed to perform obligations related to Professional Services. If Customer chooses to disclose its source code to Microsoft during a Professional Services engagement, then (1) prior to such disclosure, Customer will remove any third-party source code that Customer is prohibited from disclosing; and (2) Microsoft will treat Customer's source code as confidential information.

Services Deliverables License

"Services Deliverables" means any computer code or materials (including without limitation proofs of concept, documentation and design recommendations, sample code, software libraries, algorithms and machine learning models) other than Products or Fixes that Microsoft leaves with Customer at the conclusion of Microsoft's performance of Professional Services. Microsoft grants Customer a non-exclusive, non-transferable, perpetual license to reproduce, use, and modify the Services Deliverables, subject to and in accordance with the terms and conditions in Customer's volume licensing agreement and any agreed statement of services. Some Services Deliverables and third-party content may be provided under a separate license, such as an open source license. In the event of a conflict between this Notice and any separate license, the separate license will prevail with respect to the Services Deliverables or third-party content that is the subject of such separate license. Each party reserves all rights (and no one receives any rights) not expressly granted by the foregoing licenses.

License Restrictions

Customer must not (and is not licensed to) reverse engineer, decompile, disassemble or work around any technical limitations in any Services Deliverable except to the extent that applicable law doesn't allow this restriction. Except as expressly permitted in this agreement and any agreed statement of services or separate license, Customer must not (and is not licensed to) distribute, sublicense, rent, lease, lend, sell, offer

for sale or otherwise make available any Services Deliverables, in whole or in part, or subject Microsoft's intellectual property in Services Deliverables to any other license terms.

Feedback

"Feedback" means expertise and knowledge, including industry knowhow, as well as comments, input and suggestions regarding the Services Deliverables, Professional Services and the products, technologies, services, or any components of the foregoing, whether pre-release or commercially released, of either Microsoft or Customer. Neither Microsoft nor Customer are required to provide Feedback to the other in connection with Professional Services, but if a party in its sole discretion does provide Feedback, both parties agree that the receiving party should be free to use such Feedback without obligation. Accordingly, to the extent that the party providing Feedback owns or controls copyrights or trade secrets covering such Feedback, that party grants to the receiving party and its Affiliates a worldwide, non-exclusive, perpetual, irrevocable and royalty-free license in such intellectual property to: (1) to make, use, modify, distribute, create derivative works and otherwise commercialize the Feedback as part of Microsoft's or Customer's products, technologies, services or any of their components, including without limitation pre-release and commercially released versions of such offerings; and (2) sublicense to third parties the foregoing rights, including the right to grant further sublicenses. Neither party will provide any Feedback subject to any terms that would impose any obligation on or require attribution by on the receiving party. Any party receiving Feedback further acknowledges that (1) it has sole and absolute discretion regarding whether it implements such feedback; (2) it shall base its offerings and marketing plans solely on its own independent research and analysis; and (3) it assumes all risks associated with any implementation of such Feedback.

Non-Microsoft Technology

Customer is solely responsible for any non-Microsoft software or technology that it installs or uses with the Online Services, Fixes, or Services Deliverables, including without limitation when Customer asks Microsoft to use or modify such third-party content.

Affiliates' Rights

Customer may sublicense the rights to use Services Deliverables to its Affiliates, but Customer's Affiliates may not sublicense these rights. Customer is liable for ensuring its Affiliates' compliance with the terms of this Notice and Customer's volume licensing agreement.

Government Customers

If Customer is a government entity, then the following terms apply to any Professional Services provided at no charge to Customer. Microsoft waives any and all entitlement to compensation from Customer for the Professional Services. In compliance with applicable laws and regulations, Microsoft and Customer acknowledge that the Professional Services are for the sole benefit and use of Customer and not provided for the personal use or benefit of any individual government employee.

Table of Contents / General Terms

Notice about Azure Media Services H.265/HEVC Encoding

Customer must obtain its own patent license(s) from any third party H.265/HEVC patent pools or rights holders before using Azure Media Services to encode or decode H.265/HEVC media.

Table of Contents / General Terms

Notice about Adobe Flash Player

The software may include a version of Adobe Flash Player. Customer agrees that its use of the Adobe Flash Player is governed by the license terms for Adobe Systems Incorporated at http://go.microsoft.com/fwlink/?linkid=248532. Adobe and Flash are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Table of Contents / General Terms

Notice about H.264/AVC Visual Standard, VC-1 Video Standard, MPEG-4 Part 2 Visual Standard and MPEG-2 Video Standard

This software may include H.264/AVC, VC-1, MPEG-4 Part 2, and MPEG-2 visual compression technology. MPEG LA, L.L.C. requires this notice: THIS PRODUCT IS LICENSED UNDER THE AVC, THE VC-1, THE MPEG-4 PART 2 AND MPEG-2 VISUAL PATENT PORTFOLIO LICENSES FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE ABOVE (VIDEO STANDARDS) AND/OR (ii) DECODE AVC, VC-1, MPEG-4 PART 2 AND MPEG-2 VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE SUCH VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. REFER TO www.mpegla.com.

For clarification purposes, this notice does not limit or inhibit the use of the software for normal business uses that are personal to that business which do not include (i) redistribution of the software to third parties, or (ii) creation of content compliant with the VIDEO STANDARDS technologies for distribution to third parties.

Table of Contents / General Terms

Attachment 2 – Subscription License Suites

Online Services may be available for purchase as Suites of Online Services. If, in the tables below, a cell is shaded blue in an Online Service's row, the Suite SL for the column the cell is in fulfills the SL requirements for the cell's Online Services. For Education and Government offers, see the Public Sector table below.

Online Service	Office 365 Enterprise [1, 3]				Office 365 Business Essentials	Office 365 Business Premium	Enterprise Mobility + Security		Microsoft 365 Enterprise [2]					Microsoft 365 Business
	F3	E1	E3	E5			E3	E5	F1	F3	E3	E5	E5 Security[6]	
Exchange Online K1	■									■				
Exchange Online Plan 1		■			■	■								■
Exchange Online Plan 2			■	■							■	■		
SharePoint Online K1	■								■	■				
SharePoint Online Plan 1		■			■	■								■
SharePoint Online Plan 2			■	■							■	■		
Skype for Business Online Plan 2		■	■	■	■	■					■	■		■
OneDrive for Business Plan 1		■			■	■								■
OneDrive for Business Plan 2			■	■							■	■		
Phone System				■								■		
Audio Conferencing				■								■		
Office 365 Business						■								■
Office 365 ProPlus			■	■							■	■		
Microsoft Kaizala Pro	■	■	■	■	■	■				■	■	■		■
Office 365 Data Loss Prevention			■	■							■	■		
Office 365 Advanced Threat Protection Plan 1				■								■	■	■
Office 365 Advanced Threat Protection Plan 2				■								■	■	
Microsoft Power BI Pro				■								■		
Microsoft Intune							■	■	■	■	■	■		■
Azure Info Protection Premium Plan 1							■		■	■	■			
Azure Active Directory Premium Plan 1							■		■	■	■			
Azure Active Directory Premium Plan 2								■				■	■	
Azure Advanced Threat Protection for Users								■				■	■	
Microsoft Cloud App Security								■				■	■	
Microsoft Stream	■ [7,8]	■	■	■	■	■			■ [7,8]	■ [7,8]	■	■		■ [8]

[1] Add-on Suite SLs that include "without ProPlus" in the title do not include rights to Office 365 ProPlus.
[2] In addition to the Online Services identified above, the Microsoft 365 fulfills the SL requirement for Windows SA per User as described in the Product Terms.
[3] Inclusion of Skype for Business Online Audio Conferencing with Office 365 E5 is dependent on regional availability.
[5] Office 365 customers with 500 seats or fewer will be onboarded to Microsoft Teams and will not have access to Skype for Business Online.
[6] Microsoft 365 E5 Security includes Microsoft Defender Advanced Threat Protection.
[7] Cannot upload or modify videos.
[8] Cannot create live events.

Public Sector

Online Service	Office 365 Government[1,3]					Office 365 Education[3]			Microsoft 365 Education[2]			
	F3	E1	E3	E4	E5	A1	A3	A5	A1	A3[5]	A5	A5 Security[6]
Exchange Online K1	■											
Exchange Online Plan 1		■				■						
Exchange Online Plan 2			■	■	■		■	■		■	■	
SharePoint Online K1	■											
SharePoint Online Plan 1		■				■						
SharePoint Online Plan 2			■	■	■		■	■		■	■	
Skype for Business Online Plan 2		■	■	■	■	■	■	■		■	■	
OneDrive for Business Plan 1		■				■						
OneDrive for Business Plan 2			■	■	■		■	■		■	■	
Phone System					■			■			■	
Audio Conferencing					■			■			■	
Office 365 ProPlus			■	■	■		■	■		■	■	
Microsoft Kaizala Pro	■	■	■	■	■		■	■		■	■	
Office 365 Data Loss Prevention			■		■		■	■		■	■	
Office 365 Advanced Threat Protection P2					■			■			■	■
Microsoft Power BI Pro					■			■			■	
Office 365 Advanced Threat Protection P1					■			■			■	■
Microsoft Intune									■	■	■	
Azure Info Protection Premium Plan 1										■		
Azure Active Directory Premium Plan 1										■		
Azure Active Directory Premium Plan 2											■	■
Azure Advanced Threat Protection for Users											■	■
Microsoft Cloud App Security											■	■
Microsoft Stream					■			■			■	
Minecraft: Education Edition										■	■	

[1] *Add-on Suite SLs that include "without ProPlus" in the title do not include rights to Office 365 ProPlus.*
[2] *In addition to the Online Services identified above, the Microsoft 365 Education fulfills the SL requirement for Windows SA per User as described in the Product Terms.*
[3] *Inclusion of Skype for Business Online Audio Conferencing with Office 365 E5/A5 is dependent on regional availability.*
[4] *Includes Microsoft 365 A3 with Core CAL.*
[5] *Office 365 customers with 500 seats or fewer will be onboarded to Microsoft Teams and will not have access to Skype for Business Online.*
[6] *Microsoft 365 A5 Security includes Microsoft Defender Advanced Threat Protection.*
[7] *Cannot upload or modify videos.*
[8] *Cannot create live events.*

Table of Contents / General Terms

Volume Licensing

Microsoft Online Services Data Protection Addendum January 2020

Microsoft

Table of Contents

Introduction

The parties agree that this Microsoft Online Services Data Protection Addendum ("DPA") sets forth their obligations with respect to the processing and security of Customer Data and Personal Data in connection with the Online Services. The parties also agree that, unless a separate Professional Services agreement exists, this DPA governs the processing and security of Professional Services Data. Separate terms, including different privacy and security terms, govern Customer's use of Non-Microsoft Products.

In the event of any conflict or inconsistency between this DPA and any other terms in Customer's volume licensing agreement (including the Product Terms or the Online Services Terms), this DPA shall prevail. The provisions of this DPA supersede any conflicting provisions of the Microsoft Privacy Statement that otherwise may apply to processing of Customer Data, Personal Data, or Professional Services Data as defined herein. For clarity, consistent with Clause 10 of the Standard Contractual Clauses in Attachment 2, the Standard Contractual Clauses prevail over any other term of the DPA.

Microsoft makes the commitments in this DPA to all customers with volume license agreements. These commitments are binding on Microsoft with regard to Customer regardless of (1) the version of the OST that is otherwise applicable to any given Online Services subscription, or (2) any other agreement that references the OST.

Applicable DPA and Updates

When Customer renews or purchases a new subscription to an Online Service, the then-current DPA will apply and will not change during Customer's subscription for that Online Service. When Microsoft introduces features, supplements or related software that are new (i.e., that were not previously included with the subscription), Microsoft may provide terms or make updates to the DPA that apply to Customer's use of those new features, supplements or related software.

Electronic Notices

Microsoft may provide Customer with information and notices about Online Services electronically, including via email, through the portal for the Online Service, or through a web site that Microsoft identifies. Notice is given as of the date it is made available by Microsoft.

Prior Versions

The DPA and OST provide terms for Online Services that are currently available. For earlier versions of the DPA and the OST, Customer may refer to https://aka.ms/licensingdocs or contact its reseller or Microsoft Account Manager.

Clarifications and Summary of Changes

None

Table of Contents / General Terms

Definitions

Capitalized terms used but not defined in this DPA will have the meanings provided in the volume license agreement. The following defined terms are used in this DPA:

"Customer Data" means all data, including all text, sound, video, or image files, and software, that are provided to Microsoft by, or on behalf of, Customer through use of the Online Service. Customer Data does not include Professional Services Data.

"Diagnostic Data" means data collected or obtained by Microsoft from software that is locally installed by Customer in connection with the Online Service. Diagnostic Data may also be referred to as telemetry. Diagnostic Data does not include Customer Data, Service Generated Data, or Professional Services Data.

"Data Protection Requirements" means the GDPR, Local EU/EEA Data Protection Laws, and any applicable laws, regulations, and other legal requirements relating to (a) privacy and data security; and (b) the use, collection, retention, storage, security, disclosure, transfer, disposal, and other processing of any Personal Data.

"GDPR" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

"Local EU/EEA Data Protection Laws" means any subordinate legislation and regulation implementing the GDPR.

"GDPR Terms" means the terms in Attachment 3, under which Microsoft makes binding commitments regarding its processing of Personal Data as required by Article 28 of the 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 Data" means all data, including all text, sound, video, image files or software, that are provided to Microsoft, by or on behalf of a Customer (or that Customer authorizes Microsoft to obtain from an Online Service) or otherwise obtained or processed by or on behalf of Microsoft through an engagement with Microsoft to obtain Professional Services. Professional Services Data includes Support Data.

"Service Generated Data" means data generated or derived by Microsoft through the operation of an Online Service. Service Generated Data does not include Customer Data, Diagnostic Data, or Professional Services Data.

"Standard Contractual Clauses" means the standard data protection clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, as described in Article 46 of the GDPR and approved by the European Commission decision 2010/87/EC, dated 5 February 2010. The Standard Contractual Clauses are in Attachment 2.

"Subprocessor" means other processors used by Microsoft to process Customer Data and Personal Data, including any subcontractor that processes Customer Data and Personal Data.

"Support 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 technical support for Online Services covered under this agreement. Support Data is a subset of Professional Services Data.

Lower case terms used but not defined in this DPA, such as "personal data breach", "processing", "controller", "processor", "profiling", "personal data", and "data subject" will have the same meaning as set forth in Article 4 of the GDPR, irrespective of whether GDPR applies. The terms "data importer" and "data exporter" have the meanings given in the Standard Contractual Clauses.

General Terms

Compliance with Laws

Microsoft will comply with all laws and regulations applicable to its provision of the Online Services, including security breach notification law and Data Protection Requirements. However, Microsoft is not responsible for compliance with any laws or regulations applicable to Customer or Customer's industry that are not generally applicable to information technology service providers. Microsoft does not determine whether Customer Data includes information subject to any specific law or regulation. All Security Incidents are subject to the Security Incident Notification terms below.

Customer must comply with all laws and regulations applicable to its use of Online Services, including laws related to biometric data, confidentiality of communications, and Data Protection Requirements. Customer is responsible for determining whether the Online Services are appropriate for storage and processing of information subject to any specific law or regulation and for using the Online Services in a manner consistent with Customer's legal and regulatory obligations. Customer is responsible for responding to any request from a third party regarding Customer's use of an Online Service, such as a request to take down content under the U.S. Digital Millennium Copyright Act or other applicable laws.

Data Protection Terms

This section of the DPA includes the following subsections:

- Scope
- Nature of Processing; Ownership
- Disclosure of Processed Data
- Processing of Personal Data; GDPR
- Data Security
- Security Incident Notification
- Data Transfers and Location
- Data Retention and Deletion
- Processor Confidentiality Commitment
- Notice and Controls on Use of Subprocessors
- Educational Institutions
- CJIS Customer Agreement
- HIPAA Business Associate
- California Consumer Privacy Act (CCPA) Terms
- How to Contact Microsoft
- Appendix A – Security Measures

Scope

The terms in this DPA apply to all Online Services except any Online Services specifically identified in Attachment 1 to the OST as excluded, which are governed by the privacy and security terms in the applicable Online Service Specific Terms.

Previews may employ lesser or different privacy and security measures than those typically present in the Online Services. Unless otherwise noted, Customer should not use Previews to process Personal Data or other data that is subject to legal or regulatory compliance requirements. The following terms in this DPA do not apply to Previews: Processing of Personal Data; GDPR, Data Security, and HIPAA Business Associate.

Attachment 1 to the DPA includes the privacy and security terms for Professional Services Data, including any Personal Data therein, in connection with the provision of Professional Services. Therefore, unless expressly made applicable in Attachment 1, the terms in this DPA do not apply to the provision of Professional Services.

Nature of Data Processing; Ownership

Microsoft will use and otherwise process Customer Data and Personal Data only (a) to provide Customer the Online Services in accordance with Customer's documented instructions, and (b) for Microsoft's legitimate business operations, each as detailed and limited below. As between the parties, Customer retains all right, title and interest in and to Customer Data. Microsoft acquires no rights in Customer Data, other than the rights Customer grants to Microsoft in this section. This paragraph does not affect Microsoft's rights in software or services Microsoft licenses to Customer.

Processing to Provide Customer the Online Services

For purposes of this DPA, "to provide" an Online Service consists of:

- Delivering functional capabilities as licensed, configured, and used by Customer and its users, including providing personalized user experiences;
- Troubleshooting (preventing, detecting, and repairing problems); and
- Ongoing improvement (installing the latest updates and making improvements to user productivity, reliability, efficacy, and security).

When providing Online Services, Microsoft will not use or otherwise process Customer Data or Personal Data for: (a) user profiling, (b) advertising or similar commercial purposes, or (c) market research aimed at creating new functionalities, services, or products or any other purpose, unless such use or processing is in accordance with Customer's documented instructions.

Processing for Microsoft's Legitimate Business Operations

For purposes of this DPA, "Microsoft's legitimate business operations" consist of the following, each as incident to delivery of the Online Services to Customer: (1) billing and account management; (2) compensation (e.g., calculating employee commissions and partner incentives); (3) internal reporting and modeling (e.g., forecasting, revenue, capacity planning, product strategy); (4) combatting fraud, cybercrime, or cyber-attacks that may affect Microsoft or Microsoft Products; (5) improving the core functionality of accessibility, privacy or energy-efficiency; and (6) financial reporting and compliance with legal obligations (subject to the limitations on disclosure outlined below).

When processing for Microsoft's legitimate business operations, Microsoft will not use or otherwise process Customer Data or Personal Data for: (a) user profiling, or (b) advertising or similar commercial purposes. In addition, where Microsoft is processing this data for legitimate business operations, Microsoft will process it only for the purposes set out in this section.

Disclosure of Processed Data

Microsoft will not disclose Processed Data except: (1) as Customer directs; (2) as described in this DPA; or (3) as required by law. For purposes of this section, "Processed Data" means: (a) Customer Data; (b) Personal Data; and (c) any other data processed by Microsoft in connection with the Online Service that is Customer's confidential information under the volume license agreement. All processing of Processed Data is subject to Microsoft's obligation of confidentiality under the volume license agreement.

Microsoft will not disclose Processed Data to law enforcement unless required by law. If law enforcement contacts Microsoft with a demand for Processed Data, Microsoft will attempt to redirect the law enforcement agency to request that data directly from Customer. If compelled to disclose Processed 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 Processed 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.

Microsoft will not provide any third party: (a) direct, indirect, blanket, or unfettered access to Processed Data; (b) platform encryption keys used to secure Processed Data or the ability to break such encryption; or (c) access to Processed Data if Microsoft is aware that the data is to be used for purposes other than those stated in the third party's request.

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

Processing of Personal Data; GDPR

All Personal Data processed by Microsoft in connection with the Online Services is obtained as either Customer Data, Diagnostic Data, or Service Generated Data. Personal Data provided to Microsoft by, or on behalf of, Customer through use of the Online Service is also Customer Data. Pseudonymized identifiers may be included in Diagnostic Data or Service Generated Data and are also Personal Data. Any Personal Data pseudonymized, or de-identified but not anonymized, or Personal Data derived from Personal Data is also Personal Data.

To the extent Microsoft is a processor or subprocessor of Personal Data subject to the GDPR, the GDPR Terms in Attachment 3 govern that processing and the parties also agree to the following terms in this sub-section ("Processing of Personal Data; GDPR"):

Processor and Controller Roles and Responsibilities

Customer and Microsoft agree that Customer is the controller of Personal Data and Microsoft is the processor of such data, except (a) when Customer acts as a processor of Personal Data, in which case Microsoft is a subprocessor; or (b) as stated otherwise in the Online Service Specific terms or this DPA. When Microsoft acts as the processor or subprocessor of Personal Data, it will process Personal Data only on documented instructions from Customer. Customer agrees that its volume licensing agreement (including this DPA and the OST), along with the product documentation and Customer's use and configuration of features in the Online Services, are Customer's complete and final documented instructions to Microsoft for the processing of Personal Data. Information on use and configuration of the Online Services can be found at https://docs.microsoft.com/en-us/ or a successor location. Any additional or alternate instructions must be agreed to according to the process for amending Customer's volume licensing agreement. In any instance where the GDPR applies and Customer is a processor, Customer warrants to Microsoft that Customer's instructions, including appointment of Microsoft as a processor or subprocessor, have been authorized by the relevant controller.

To the extent Microsoft uses or otherwise processes Personal Data subject to the GDPR or other Data Protection Requirements in connection with Microsoft's legitimate business operations, Microsoft will be an independent data controller for such use and will be responsible for complying with all applicable laws and controller obligations. Microsoft employs safeguards to protect Customer Data and Personal Data in processing, including those identified in this DPA and those contemplated in Article 6(4) of the GDPR.

Processing Details

The parties acknowledge and agree that:

- **Subject Matter.** The subject-matter of the processing is limited to Personal Data within the scope of the section of this DPA entitled "Nature of Data Processing; Ownership" above and the GDPR.
- **Duration of the Processing.** The duration of the processing shall be in accordance with Customer instructions and the terms of the DPA.
- **Nature and Purpose of the Processing.** The nature and purpose of the processing shall be to provide the Online Service pursuant to Customer's volume licensing agreement (as further described in the section of this DPA entitled "Nature of Data Processing; Ownership" above).
- **Categories of Data.** The types of Personal Data processed by the Online Service include: (i) Personal Data that Customer elects to include in Customer Data; and (ii) those expressly identified in Article 4 of the GDPR that may be contained in Diagnostic Data or Service Generated Data. The types of Personal Data that Customer elects to include in Customer Data may be any categories of Personal Data identified in records maintained by Customer acting as controller pursuant to Article 30 of the GDPR, including the categories of Personal Data set forth in Appendix 1 to Attachment 2 – The Standard Contractual Clauses (Processors) of the DPA.
- **Data Subjects.** The categories of data subjects are Customer's representatives and end users, such as employees, contractors, collaborators, and customers, and may include any other categories of data subjects as identified in records maintained by Customer acting as controller pursuant to Article 30 of the GDPR, including the categories of data subjects set forth in Appendix 1 to Attachment 2 – The Standard Contractual Clauses (Processors) of the DPA.

Data Subject Rights; Assistance with Requests

Microsoft will make available to Customer, in a manner consistent with the functionality of the Online Service and Microsoft's role as a processor of Personal Data of data subjects, the ability to fulfill data subject requests to exercise their rights under the GDPR. If Microsoft receives a request from Customer's data subject to exercise one or more of its rights under the GDPR in connection with an Online Service for which Microsoft is a data processor or subprocessor, Microsoft will redirect the data subject to make its request directly to Customer. Customer will be responsible for responding to any such request including, where necessary, by using the functionality of the Online Service. Microsoft shall comply with reasonable requests by Customer to assist with Customer's response to such a data subject request.

Records of Processing Activities

To the extent the GDPR requires Microsoft to collect and maintain records of certain information relating to Customer, Customer will, where requested, supply such information to Microsoft and keep it accurate and up-to-date. Microsoft may make any such information available to the supervisory authority if required by the GDPR.

Data Security

Security Practices and Policies

Microsoft will implement and maintain appropriate technical and organizational measures to protect Customer Data and Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. Those measures shall be set forth in a Microsoft Security Policy. Microsoft will make that policy available to Customer, along with descriptions of the security controls in place for the Online Service and other information reasonably requested by Customer regarding Microsoft security practices and policies.

In addition, those measures shall comply with the requirements set forth in ISO 27001, ISO 27002, and ISO 27018. Each Core Online Service also complies with the control standards and frameworks shown in the table in Attachment 1 to the OST and implements and maintains the security measures set forth in Appendix A for the protection of Customer Data.

Microsoft may add industry or government standards at any time. Microsoft will not eliminate ISO 27001, ISO 27002, ISO 27018 or the standards or frameworks in the table in Attachment 1 to the OST, unless it is no longer used in the industry and it is replaced with a successor (if any).

Customer Responsibilities

Customer is solely responsible for making an independent determination as to whether the technical and organizational measures for an Online Service meet Customer's requirements, including any of its security obligations under applicable Data Protection Requirements. Customer acknowledges and agrees that (taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing of its Personal Data as well as the risks to individuals) the security practices and policies implemented and maintained by Microsoft provide a level of security appropriate to the risk with respect to its Personal Data. Customer is responsible for implementing and maintaining privacy protections and security measures for components that Customer provides or controls (such as devices enrolled with Microsoft Intune or within a Microsoft Azure customer's virtual machine or application).

Auditing Compliance

Microsoft will conduct audits of the security of the computers, computing environment and physical data centers that it uses in processing Customer Data and Personal Data, as follows:

- Where a standard or framework provides for audits, an audit of such control standard or framework will be initiated at least annually.
- Each audit will be performed according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework.
- Each audit will be performed by qualified, independent, third party security auditors at Microsoft's selection and expense.

Each audit will result in the generation of an audit report ("Microsoft Audit Report"), which Microsoft will make available at https://servicetrust.microsoft.com/ or another location identified by Microsoft. The Microsoft Audit Report will be Microsoft's Confidential Information and will clearly disclose any material findings by the auditor. Microsoft will promptly remediate issues raised in any Microsoft Audit Report to the satisfaction of the auditor. If Customer requests, Microsoft will provide Customer with each Microsoft Audit Report. The Microsoft Audit Report will be subject to non-disclosure and distribution limitations of Microsoft and the auditor.

To the extent Customer's audit requirements under the Standard Contractual Clauses or Data Protection Requirements cannot reasonably be satisfied through audit reports, documentation or compliance information Microsoft makes generally available to its customers, Microsoft will promptly respond to Customer's additional audit instructions. Before the commencement of an audit, Customer and Microsoft will mutually agree upon the scope, timing, duration, control and evidence requirements, and fees for the audit, provided that this requirement to agree will not permit Microsoft to unreasonably delay performance of the audit. To the extent needed to perform the audit, Microsoft will make the processing systems, facilities and supporting documentation relevant to the processing of Customer Data and Personal Data by Microsoft, its Affiliates, and its Subprocessors available. Such an audit will be conducted by an independent, accredited third-party audit firm, during regular business hours, with reasonable advance notice to Microsoft, and subject to reasonable confidentiality procedures. Neither Customer nor the auditor shall have access to any data from Microsoft's other customers or to Microsoft systems or facilities not involved in the Online Services. Customer is responsible for all costs and fees related to such audit, including all reasonable costs and fees for any and all time Microsoft expends for any such audit, in addition to the rates for services performed by Microsoft. If the audit report generated as a result of Customer's audit includes any finding of material non-compliance, Customer shall share such audit report with Microsoft and Microsoft shall promptly cure any material non-compliance.

If the Standard Contractual Clauses apply, then this section is in addition to Clause 5 paragraph f and Clause 12 paragraph 2 of the Standard Contractual Clauses. Nothing in this section of the DPA varies or modifies the Standard Contractual Clauses or the GDPR Terms or affects any supervisory authority's or data subject's rights under the Standard Contractual Clauses or Data Protection Requirements. Microsoft Corporation is an intended third-party beneficiary of this section.

Security Incident Notification

If Microsoft becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data or Personal Data while processed by Microsoft (each a "Security Incident"), Microsoft will promptly and without undue delay (1) notify Customer of the Security Incident; (2) investigate the Security Incident and provide Customer with detailed information about the Security Incident; (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

Notification(s) of Security Incidents will be delivered to one or more of Customer's administrators by any means Microsoft selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information on each applicable Online Services portal. Customer is solely responsible for complying with its obligations under incident notification laws applicable to Customer and fulfilling any third-party notification obligations related to any Security Incident.

Microsoft shall make reasonable efforts to assist Customer in fulfilling Customer's obligation under GDPR Article 33 or other applicable law or regulation to notify the relevant supervisory authority and data subjects about such Security Incident.

Microsoft's notification of or response to a Security Incident under this section is not an acknowledgement by Microsoft of any fault or liability with respect to the Security Incident.

Customer must notify Microsoft promptly about any possible misuse of its accounts or authentication credentials or any security incident related to an Online Service.

Data Transfers and Location

Data Transfers

Except as described elsewhere in the DPA, Customer Data and Personal 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 Subprocessors operate. Customer appoints Microsoft to perform any such transfer of Customer Data and Personal Data to any such country and to store and process Customer Data and Personal Data to provide the Online Services.

All transfers of Customer Data out of the European Union, European Economic Area, and Switzerland by the Core Online Services shall be governed by the Standard Contractual Clauses in Attachment 3, unless the Customer has opted out of those clauses.

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. All transfers of Personal Data to a third country or an international organization will be subject to appropriate safeguards as described in Article 46 of the GDPR and such transfers and safeguards will be documented according to Article 30(2) of the GDPR.

In addition, 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 if 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.

Location of Customer Data at Rest

For the Core Online Services, Microsoft will store Customer Data at rest within certain major geographic areas (each, a Geo) as set forth in Attachment 1 to the OST.

Microsoft does not control or limit the regions from which Customer or Customer's end users may access or move Customer Data.

Data Retention and Deletion

At all times during the term of Customer's subscription, Customer will have the ability to access, extract and delete Customer Data stored in each Online Service.

Except for free trials and LinkedIn services, Microsoft will retain Customer Data that remains stored in Online Services in a limited function account for 90 days after expiration or termination of Customer's subscription so that Customer may extract the data. After the 90-day retention period ends, Microsoft will disable Customer's account and delete the Customer Data and Personal Data within an additional 90 days, unless Microsoft is permitted or required by applicable law, or authorized under this DPA, to retain such data.

The Online Service may not support retention or extraction of software provided by Customer. Microsoft has no liability for the deletion of Customer Data or Personal Data as described in this section.

Processor Confidentiality Commitment

Microsoft will ensure that its personnel engaged in the processing of Customer Data and Personal Data (i) will process such data only on instructions from Customer or as described in this DPA, and (ii) will be obligated to maintain the confidentiality and security of such data even after their engagement ends. Microsoft shall provide periodic and mandatory data privacy and security training and awareness to its employees with access to Customer Data and Personal Data in accordance with applicable Data Protection Requirements and industry standards.

Notice and Controls on use of Subprocessors

Microsoft may hire third parties to provide certain limited or ancillary services on its behalf. Customer consents to the engagement of these third parties and Microsoft Affiliates as Subprocessors. The above authorizations will constitute Customer's prior written consent to the subcontracting by Microsoft of the processing of Customer Data and Personal Data if such consent is required under the Standard Contractual Clauses or the GDPR Terms.

Microsoft is responsible for its Subprocessors' compliance with Microsoft's obligations in this DPA. Microsoft makes available information about Subprocessors on a Microsoft website. When engaging any Subprocessor, Microsoft will ensure via a written contract that the Subprocessor may access and use Customer Data or Personal Data only to deliver the services Microsoft has retained them to provide and is prohibited from using Customer Data or Personal Data for any other purpose. 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 the DPA. Microsoft agrees to oversee the Subprocessors to ensure that these contractual obligations are met.

From time to time, Microsoft may engage new Subprocessors. Microsoft will give Customer notice (by updating the website and providing Customer with a mechanism to obtain notice of that update) of any new Subprocessor at least 6 months in advance of providing that Subprocessor with access to Customer Data. Additionally, Microsoft will give Customer notice (by updating the website and providing Customer with a mechanism to obtain notice of that update) of any new Subprocessor at least 14 days in advance of providing that Subprocessor with access to Personal Data other than that which is contained in Customer Data.

If Customer does not approve of a new Subprocessor, then Customer may terminate any subscription for the affected Online Service without penalty by providing, before the end of the relevant notice period, written notice of termination. Customer may also include an explanation of the grounds for non-approval together with the termination notice, in order to permit Microsoft to re-evaluate any such new Subprocessor based on the applicable concerns. If the affected Online Service is part of a suite (or similar single purchase of services), then any termination will apply to the entire suite. After termination, Microsoft will remove payment obligations for any subscriptions for the terminated Online Service from subsequent invoices to Customer or its reseller.

Educational Institutions

If Customer is an educational agency or institution to which regulations under the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (FERPA), apply, Microsoft acknowledges that for the purposes of the DPA, Microsoft is a "school official" with "legitimate educational interests" in the Customer Data, as those terms have been defined under FERPA and its implementing regulations, and Microsoft agrees to abide by the limitations and requirements imposed by 34 CFR 99.33(a) on school officials.

Customer understands that Microsoft may possess limited or no contact information for Customer's students and students' parents. Consequently, Customer will be responsible for obtaining any parental consent for any end user's use of the Online Service that may be required by applicable law and to convey notification on behalf of Microsoft to students (or, with respect to a student under 18 years of age and not in attendance at a postsecondary institution, to the student's parent) of any judicial order or lawfully-issued subpoena requiring the disclosure of Customer Data in Microsoft's possession as may be required under applicable law.

CJIS Customer Agreement

Microsoft provides certain government cloud services ("Covered Services") in accordance with the FBI Criminal Justice Information Services ("CJIS") Security Policy ("CJIS Policy"). The CJIS Policy governs the use and transmission of criminal justice information. All Microsoft CJIS Covered Services shall be governed by the terms and conditions in the CJIS Customer Agreement located here: http://aka.ms/CJISCustomerAgreement.

HIPAA Business Associate

If Customer is a "covered entity" or a "business associate" and includes "protected health information" in Customer Data as those terms are defined in 45 CFR § 160.103, execution of Customer's volume licensing agreement includes execution of the HIPAA Business Associate Agreement ("BAA"), the full text of which identifies the Online Services to which it applies and is available at http://aka.ms/BAA. Customer may opt out of the BAA by sending the following information to Microsoft in a written notice (under the terms of the Customer's volume licensing agreement):

- the full legal name of the Customer and any Affiliate that is opting out; and
- if Customer has multiple volume licensing agreements, the volume licensing agreement to which the opt out applies.

California Consumer Privacy Act (CCPA)

If Microsoft is processing Personal Data within the scope of the CCPA, Microsoft makes the following additional commitments to Customer. Microsoft will process Customer Data and Personal Data on behalf of Customer and, not retain, use, or disclose that data for any purpose other than for the purposes set out in this DPA and as permitted under the CCPA, including under any "sale" exemption. In no event will Microsoft sell any such data. These CCPA terms do not limit or reduce any data protection commitments Microsoft makes to Customer in the DPA, Online Services Terms, or other agreement between Microsoft and Customer.

How to Contact Microsoft

If Customer believes that Microsoft is not adhering to its privacy or security commitments, Customer may contact customer support or use Microsoft's Privacy web form, located at http://go.microsoft.com/?linkid=9846224. Microsoft's mailing address is:

Microsoft Enterprise Service Privacy
Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052 USA

Microsoft Ireland Operations Limited is Microsoft's data protection representative for the European Economic Area and Switzerland. The privacy representative of Microsoft Ireland Operations Limited 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

Appendix A – Security Measures

Microsoft has implemented and will maintain for Customer Data in the Core Online Services the following security measures, which in conjunction with the security commitments in this DPA (including the GDPR Terms), are Microsoft's only responsibility with respect to the security of that data.

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. **Security Roles and Responsibilities**. Microsoft personnel with access to Customer Data are subject to confidentiality obligations. **Risk Management Program**. Microsoft performed a risk assessment before processing the Customer Data or launching the Online Services service. 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 Customer Data is stored. Access to the inventories of such media is restricted to Microsoft personnel authorized in writing to have such access. **Asset Handling** - Microsoft classifies Customer Data to help identify it and to allow for access to it to be appropriately restricted. - Microsoft imposes restrictions on printing Customer Data and has procedures for disposing of printed materials that contain Customer Data. - Microsoft personnel must obtain Microsoft authorization prior to storing Customer Data on portable devices, remotely accessing Customer Data, or processing Customer 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 Customer Data are located to identified authorized individuals. **Physical Access to Components**. Microsoft maintains records of the incoming and outgoing media containing Customer Data, including the kind of media, the authorized sender/recipients, date and time, the number of media and the types of Customer Data they contain. **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. **Component Disposal**. Microsoft uses industry standard processes to delete Customer 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 Customer Data. **Data Recovery Procedures** - On an ongoing basis, but in no case less frequently than once a week (unless no Customer Data has been updated during that period), Microsoft maintains multiple copies of Customer Data from which Customer Data can be recovered. - Microsoft stores copies of Customer Data and data recovery procedures in a different place from where the primary computer equipment processing the Customer Data is located. - Microsoft has specific procedures in place governing access to copies of Customer Data. - Microsoft reviews data recovery procedures at least every six months, except for data recovery procedures for Azure Government Services, which are reviewed every twelve months. - 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. **Malicious Software**. Microsoft has anti-malware controls to help avoid malicious software gaining unauthorized access to Customer Data, including malicious software originating from public networks. **Data Beyond Boundaries**

Domain	Practices
	- Microsoft encrypts, or enables Customer to encrypt, Customer Data that is transmitted over public networks. - Microsoft restricts access to Customer Data in media leaving its facilities. **Event Logging**. Microsoft logs, or enables Customer to log, access and use of information systems containing Customer 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 Customer Data. **Access Authorization** - Microsoft maintains and updates a record of personnel authorized to access Microsoft systems that contain Customer Data. - Microsoft deactivates authentication credentials that have not been used for a period of time not to exceed six months. - Microsoft identifies those personnel who may grant, alter or cancel authorized access to data and resources. - Microsoft ensures that where more than one individual has access to systems containing Customer Data, the individuals have separate identifiers/log-ins. **Least Privilege** - Technical support personnel are only permitted to have access to Customer Data when needed. - Microsoft restricts access to Customer Data to only those individuals who require such access to perform their job function. **Integrity and Confidentiality** - Microsoft instructs Microsoft personnel to disable administrative sessions when leaving premises Microsoft controls or when computers are otherwise left unattended. - Microsoft stores passwords in a way that makes them unintelligible while they are in force. **Authentication** - Microsoft uses industry standard practices to identify and authenticate users who attempt to access information systems. - Where authentication mechanisms are based on passwords, Microsoft requires that the passwords are renewed regularly. - Where authentication mechanisms are based on passwords, Microsoft requires the password to be at least eight characters long. - Microsoft ensures that de-activated or expired identifiers are not granted to other individuals. - Microsoft monitors, or enables Customer to monitor, repeated attempts to gain access to the information system using an invalid password. - Microsoft maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed. - 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. **Network Design**. Microsoft has controls to avoid individuals assuming access rights they have not been assigned to gain access to Customer Data they are not authorized to access.
Information Security Incident Management	**Incident Response Process** - 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. - For each security breach that is a Security Incident, notification by Microsoft (as described in the "Security Incident Notification" section above) will be made without undue delay and, in any event, within 72 hours. - Microsoft tracks, or enables Customer to track, disclosures of Customer Data, including what data has been disclosed, to whom, and at what time. **Service Monitoring**. Microsoft security personnel verify logs at least every six months to propose remediation efforts if necessary.

Domain	Practices
Business Continuity Management	- Microsoft maintains emergency and contingency plans for the facilities in which Microsoft information systems that process Customer Data are located. - Microsoft's redundant storage and its procedures for recovering data are designed to attempt to reconstruct Customer Data in its original or last-replicated state from before the time it was lost or destroyed.

Table of Contents / General Terms

Attachment 1 – Notices

Professional Services

Professional Services are provided subject to the "Professional Services Terms" below. If, however, Professional Services are provided pursuant to a separate agreement, then the terms of that separate agreement will apply to those Professional Services.

The Professional Services to which this Notice applies are not Online Services, and the rest of the Online Services Terms and DPA do not apply unless expressly made applicable by the Professional Services Terms below.

Processing of Professional Services Data; Ownership

Microsoft will use and otherwise process Professional Services Data only (a) to provide Customer the Professional Services in accordance with the Customer's documented instructions, and (b) for Microsoft's legitimate business operations, each as detailed and limited below. As between the parties, Customer retains all right, title and interest in and to Professional Services Data. Microsoft acquires no rights in Professional Services Data, other than the rights Customer grants to Microsoft to provide the Professional Services to Customer. This paragraph does not affect Microsoft's rights in software or services Microsoft licenses to Customer.

Processing to Provide Customer the Professional Services

For purposes of this DPA, "to provide" Professional Services consists of:

- Delivering the Professional Services, including providing technical support, professional planning, advice, guidance, data migration, deployment, and solution/software development services;
- Troubleshooting (preventing, detecting, investigating, mitigating, and repairing problems, including Security Incidents); and
- Ongoing improvement (maintaining the Professional Services, including installing the latest updates, and making improvements to the reliability, efficacy, quality, and security).

When providing Professional Services, Microsoft will not use or otherwise process Professional Services Data for: (a) user profiling, (b) advertising or similar commercial purposes, or (c) market research aimed at creating new functionalities, services, or products or any other purpose, unless such use or processing is in accordance with Customer's documented instructions.

Processing for Microsoft's Legitimate Business Operations

For purposes of this DPA, "Microsoft's legitimate business operations" consist of: (1) billing and account management; (2) compensation (e.g., calculating employee commissions); (3) internal reporting and modeling (e.g., forecasting, revenue, capacity planning, product strategy); (4) combatting fraud, cybercrime, or cyber-attacks that may affect Microsoft or Microsoft Products; (5) improving the core functionality of accessibility, privacy or energy-efficiency; and (6) financial reporting or compliance with legal obligations (subject to the limitations on disclosure outlined below), each incident to the delivery of the Professional Services to Customer.

When processing for Microsoft's legitimate business operations, Microsoft will not use or otherwise process Professional Services Data for: (a) user profiling, or (b) advertising or similar commercial purposes.

Disclosure of Professional Services Data

The "Disclosure of Processed Data" provision of the Data Protection Terms section of the OST applies to Customer's Professional Services engagement with respect to Professional Services Data.

Processing of Personal Data; GDPR

Personal Data provided to Microsoft by, or on behalf of, Customer through an engagement with Microsoft to obtain Professional Services is also Professional Services Data.

To the extent Microsoft is a processor or subprocessor of Personal Data subject to the GDPR, the GDPR Terms in Attachment 3 govern that processing and the parties also agree to the following terms in this sub-section ("Processing of Personal Data; GDPR"):

Processor and Controller Roles and Responsibilities

Customer and Microsoft agree that Customer is the controller of Personal Data included in Professional Services Data and Microsoft is the processor, except (a) when Customer acts as a processor of Personal Data, in which case Microsoft is a subprocessor; or (b) as stated otherwise in these Professional Services Terms. When Microsoft acts as the processor or subprocessor of Personal Data, it will process Personal Data only on documented instructions from Customer. Customer agrees that its volume licensing agreement (including this DPA and the OST), along with any statement of services agreed between the parties, are Customer's complete and final documented instructions to Microsoft for the processing of Personal Data contained within Professional Services Data. Any additional or alternate instructions must be agreed to according to the process for amending Customer's volume licensing agreement or statements of services. In any instance where the GDPR applies and Customer is a

processor, Customer warrants to Microsoft that Customer's instructions, including appointment of Microsoft as a processor or subprocessor, have been authorized by the relevant controller.

To the extent Microsoft uses or otherwise processes Professional Services Data subject to the GDPR or other Data Protection Requirements in connection with Microsoft's legitimate business operations, Microsoft will be an independent data controller for such use and will be responsible for complying with all applicable laws and controller obligations. Microsoft employs safeguards to protect Professional Service Data in processing, including those identified in this DPA and those contemplated in Article 6(4) of the GDPR.

Processing Details

The parties acknowledge and agree that:

- **Subject Matter.** The subject-matter of the processing is limited to Personal Data within the scope of the section of these Professional Services Terms entitled "Processing of Professional Services Data; Ownership" above and the GDPR.
- **Duration of the Processing.** The duration of the processing shall be in accordance with Customer instructions and these Professional Services Terms.
- **Nature and Purpose of the Processing.** The nature and purpose of the processing shall be to provide Professional Services pursuant to Customer's volume licensing agreement and any statement of services (as further described in the section of these Professional Services Terms entitled "Processing of Professional Services Data; Ownership" above).
- **Categories of Data.** The types of Personal Data processed in connection with the provision of Professional Services include (i) Personal Data that Customer elects to include in Professional Services Data; and (ii) those expressly identified in Article 4 of the GDPR. The types of Personal Data that Customer elects to include in Professional Services Data may be any categories of Personal Data identified in records maintained by Customer acting as controller pursuant to Article 30 of the GDPR, including the categories of Personal Data set forth in Appendix 1 to Attachment 2 – The Standard Contractual Clauses (Processors) of the DPA.
- **Data Subjects.** The categories of data subjects are Customer's representatives and end users, such as employees, contractors, collaborators, and customers, and may include any other categories of data subjects as identified in records maintained by Customer acting as controller pursuant to Article 30 of the GDPR, including the categories of data subjects set forth in Appendix 1 to Attachment 2 – The Standard Contractual Clauses (Processors) of the DPA).

Data Subject Rights; Assistance with Requests

For Professional Services Data that Customer stores in an Online Service, Microsoft will abide by the obligations set forth in the "Data Subject Rights; Assistance with Requests" provision of the Data Protection Terms section of the DPA. For other Professional Services Data, Microsoft will delete or return all copies of Professional Services Data in accordance with the "Data Deletion or Return" section below.

Records of Processing Activities

To the extent the GDPR requires Microsoft to collect and maintain records of certain information relating to Customer, Customer will, where requested, supply such information to Microsoft and keep it accurate and up-to-date. Microsoft may make any such information available to the supervisory authority if required by the GDPR.

Data Security

Security Practices and Policies

Microsoft will implement and maintain appropriate technical and organizational measures to protect Professional Services Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed Those measures shall be set forth in a Microsoft Security Policy. Microsoft will make that policy available to Customer, along with other information reasonably requested by Customer regarding Microsoft security practices and policies.

Customer Responsibilities

The "Customer Responsibilities" provision of the Data Protection Terms section of the DPA applies to Customer's Professional Services engagement with respect to Professional Services Data. In addition, with respect to Customer's Professional Services engagement, Customer agrees not to provide any Professional Services Data, other than Support Data, to Microsoft which would be subject to regulations under the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (FERPA) or the Health Insurance Portability and Accountability Act of 1996 (Pub. L. 104-191) (HIPAA).

Security Incident Notification

The "Security Incident Notification" provision of the Data Protection Terms section of the DPA applies to Customer's Professional Services engagement with respect to Professional Services Data.

Data Transfers

With respect to Professional Services Data, Microsoft makes the commitments applicable to Personal Data in the "Data Transfers" provision of the Data Protection Terms section of the DPA.

Data Deletion or Return

Microsoft will delete or return all copies of Professional Services Data after the business purposes for which the Professional Services Data was collected or transferred have been fulfilled or earlier upon Customer's request, unless Microsoft is permitted or required by applicable law, or authorized under this DPA, to retain such data.

Processor Confidentiality Commitment

Microsoft will ensure that its personnel engaged in the processing of Professional Services Data (i) will process such data only on instructions from Customer or as described in these Professional Services Terms, and (ii) will be obligated to maintain the confidentiality and security of such data even after their engagement ends. Microsoft shall provide periodic and mandatory data privacy and security training and awareness to its employees with access to Professional Services Data in accordance with applicable Data Protection Requirements and industry standards.

Notice and Controls on use of Subprocessors

Microsoft may hire third parties to provide certain limited or ancillary services on its behalf. Customer consents to the engagement of these third parties and Microsoft Affiliates as Subprocessors. The above authorizations will constitute Customer's prior written consent to the subcontracting by Microsoft of the processing of Professional Services Data if such consent is required under the Standard Contractual Clauses or the GDPR Terms.

Microsoft is responsible for its Subprocessors of Professional Services Data compliance with Microsoft's obligations in Attachment 1 of the DPA. Microsoft will ensure via a written contract that the Subprocessor may access and use Professional Services Data only to deliver the services Microsoft has retained them to provide and is prohibited from using Professional Services Data for any other purpose. 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 Professional Services Terms. Microsoft agrees to oversee the Subrpocessors to ensure that these contractual obligations are met.

With respect to Professional Services Data other than Support Data, a list of Microsoft's Subprocessors is available upon request. If such list is requested, at least 30 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.

If Customer does not approve of a new Subprocessor, then Customer may terminate the affected Professional Services engagement by providing, before the end of the notice period, written notice of termination. Customer may also include an explanation of the grounds for non-approval together with the termination notice, in order to permit Microsoft to re-evaluate any such new Subprocessor based on the applicable concerns.

With respect to Support Data, Microsoft's use of Subprocessors in connection with the provision of technical support for Online Services is governed by the same restrictions and procedures that govern its use of Subprocessors in connection with the Online Services set forth in the "Notice and Controls on use of Subprocessors" provision in the DPA.

Additional Terms for Support Data

Security of Support Data

Microsoft will implement and maintain appropriate technical and organizational measures to protect Support Data. Those measures shall comply with the requirements set forth in ISO 27001, ISO 27002, and ISO 27018

Educational Institutions

Microsoft's acknowledgements and agreements and Customer's responsibilities to obtain parental consent and convey notification set out in the "Educational Institutions" provision in the Data Protection Terms section of the DPA also apply with respect to Support Data.

California Consumer Privacy Act (CCPA)

If Microsoft is processing Personal Data within the scope of the CCPA, Microsoft makes the following additional commitments to Customer. Microsoft will process Professional Services Data and Personal Data on behalf of Customer and, not retain, use, or disclose that data for any purpose other than for the purposes set out in this DPA and as permitted under the CCPA, including under any "sale" exemption. In no event will Microsoft sell any such data. These CCPA terms do not limit or reduce any data protection commitments Microsoft makes to Customer in the DPA, Online Services Terms, or other agreement between Microsoft and Customer.

Table of Contents / General Terms

Attachment 2 – The Standard Contractual Clauses (Processors)

Execution of the volume licensing agreement by Customer includes execution of this Attachment 2, which is countersigned by Microsoft Corporation. To opt out of the "Standard Contractual Clauses", Customer must send the following information to Microsoft in a written notice (under terms of the Customer's volume licensing agreement):

- the full legal name of the Customer and any Affiliate that is opting out;
- if Customer has multiple volume licensing agreements, the volume licensing agreement to which the Opt Out applies; and
- a statement that Customer (or Affiliate) opts out of the Standard Contractual Clauses.

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.

Beginning May 25, 2018 and thereafter, references to various Articles from the Directive 95/46/EC in the Standard Contractual Clauses below will be treated as references to the relevant and appropriate Articles in the GDPR.

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

Data exporter: Customer is the data exporter. The data exporter is a user of Online Services as defined in the DPA and OST.

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. Microsoft acknowledges that, depending on Customer's use of the Online Service, Customer may elect to include personal data from any of the following types of data subjects in the Customer Data:

- Employees, contractors and temporary workers (current, former, prospective) of data exporter;
- Dependents of the above;
- Data exporter's collaborators/contact persons (natural persons) or employees, contractors or temporary workers of legal entity collaborators/contact persons (current, prospective, former);
- Users (e.g., customers, clients, patients, visitors, etc.) and other data subjects that are users of data exporter's services;
- Partners, stakeholders or individuals who actively collaborate, communicate or otherwise interact with employees of the data exporter and/or use communication tools such as apps and websites provided by the data exporter;
- Stakeholders or individuals who passively interact with data exporter (e.g., because they are the subject of an investigation, research or mentioned in documents or correspondence from or to the data exporter);
- Minors; or
- Professionals with professional privilege (e.g., doctors, lawyers, notaries, religious workers, etc.).

Categories of data: The personal data transferred that is included in e-mail, documents and other data in an electronic form in the context of the Online Services. Microsoft acknowledges that, depending on Customer's use of the Online Service, Customer may elect to include personal data from any of the following categories in the Customer Data:

- Basic personal data (for example place of birth, street name and house number (address), postal code, city of residence, country of residence, mobile phone number, first name, last name, initials, email address, gender, date of birth), including basic personal data about family members and children;
- Authentication data (for example user name, password or PIN code, security question, audit trail);
- Contact information (for example addresses, email, phone numbers, social media identifiers; emergency contact details);
- Unique identification numbers and signatures (for example Social Security number, bank account number, passport and ID card number, driver's license number and vehicle registration data, IP addresses, employee number, student number, patient number, signature, unique identifier in tracking cookies or similar technology);
- Pseudonymous identifiers;
- Financial and insurance information (for example insurance number, bank account name and number, credit card name and number, invoice number, income, type of assurance, payment behavior, creditworthiness);
- Commercial Information (for example history of purchases, special offers, subscription information, payment history);
- Biometric Information (for example DNA, fingerprints and iris scans);
- Location data (for example, Cell ID, geo-location network data, location by start call/end of the call. Location data derived from use of wifi access points);
- Photos, video and audio;
- Internet activity (for example browsing history, search history, reading, television viewing, radio listening activities);
- Device identification (for example IMEI-number, SIM card number, MAC address);
- Profiling (for example based on observed criminal or anti-social behavior or pseudonymous profiles based on visited URLs, click streams, browsing logs, IP-addresses, domains, apps installed, or profiles based on marketing preferences);
- HR and recruitment data (for example declaration of employment status, recruitment information (such as curriculum vitae, employment history, education history details), job and position data, including worked hours, assessments and salary, work permit details, availability, terms of employment, tax details, payment details, insurance details and location and organizations);
- Education data (for example education history, current education, grades and results, highest degree achieved, learning disability);
- Citizenship and residency information (for example citizenship, naturalization status, marital status, nationality, immigration status, passport data, details of residency or work permit);
- Information processed for the performance of a task carried out in the public interest or in the exercise of an official authority;
- Special categories of data (for example racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, data concerning a natural person's sex life or sexual orientation, or data relating to criminal convictions or offences); or
- Any other personal data identified in Article 4 of the GDPR.

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 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 Online Services.

b. Scope and Purpose of Data Processing. The scope and purpose of processing personal data is described in the "Processing of Personal Data; GDPR" section of the DPA. The data importer operates a global network of data centers and management/support facilities, and processing may take place in any jurisdiction where data importer or its sub-processors operate such facilities in accordance with the "Security Practices and Policies" section of the DPA.

c. Customer Data Access. For the term designated under the applicable volume licensing agreement data importer will at its election and as necessary under applicable law implementing Article 12(b) of the EU Data Protection Directive, either: (1) provide data exporter with the ability to correct, delete, or block Customer Data, or (2) make such corrections, deletions, or blockages on its behalf.

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

e. Customer Data Deletion or Return. Upon expiration or termination of data exporter's use of Online Services, it may extract Customer Data and data importer will delete Customer Data, each in accordance with the OST and DPA applicable to the agreement.

Subcontractors: In accordance with the DPA, the data importer may hire other companies to provide limited services on data importer's behalf, such as providing customer support. Any such subcontractors will be permitted to obtain Customer Data only to deliver the services the data importer has retained them to provide, and they are prohibited from using Customer Data for any other purpose.

Appendix 2 to the Standard Contractual Clauses

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 Customer Data without authorization. Personnel are obligated to maintain the confidentiality of any Customer 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 Customer Data, as defined in the Security Practices and Policies section of the DPA, 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 the Security Practices and Policies section of the DPA 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, Appendix 1 and Appendix 2 on behalf of the data importer:

Signature 851B7BFC2840456 Rajesh Jha DocuSigned By: Rajesh Jha

Rajesh Jha, Corporate Vice President

Microsoft Corporation

One Microsoft Way, Redmond WA, USA 98052

Attachment 3 – European Union General Data Protection Regulation Terms

Microsoft makes the commitments in these GDPR Terms, to all customers effective May 25, 2018. These commitments are binding upon Microsoft with regard to Customer regardless of (1) the version of the OST and DPA that is otherwise applicable to any given Online Services subscription or (2) any other agreement that references this attachment.

For purposes of these GDPR Terms, Customer and Microsoft agree that Customer is the controller of 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. These GDPR Terms apply to the processing of Personal Data, within the scope of the GDPR, by Microsoft on behalf of Customer. These GDPR Terms do not limit or reduce any data protection commitments Microsoft makes to Customer in the Online Services Terms or other agreement between Microsoft and Customer. These GDPR Terms do not apply where Microsoft is a controller of Personal Data.

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 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 1 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 notification will include that information a processor must provide to a controller under Article 33(3) to the extent such information is reasonably available to Microsoft.

Table of Contents / General Terms