Volume Licensing

Online Services Terms
April 1, 2018

Microsoft

Table of Contents

INTRODUCTION 3

Service Level Agreements 3
Applicable Online Services Terms and Updates 3
Electronic Notices 3
Prior Versions 3
CLARIFICATIONS AND SUMMARY OF CHANGES 3

DEFINITIONS 4

GENERAL TERMS 5

Licensing the Online Services 5
Using the Online Services 5
Use of Software with the Online Service 5
Technical Limitations 6
Import/Export Services 6
Font Components 6
Changes to and Availability of the Online Services 6
Compliance with Laws 6
Other 6

DATA PROTECTION TERMS 7

Scope 7
Processing of Customer Data; Ownership 7
Disclosure of Customer Data 7
Processing of Personal Data; GDPR 7
Data Security 8
Security Incident Notification 9
Data Transfers and Location 10
Data Retention and Deletion 10
Processor Confidentiality Commitment 11
Notice and Controls on use of Subprocessors 11
Educational Institutions 11
HIPAA Business Associate 11
How to Contact Microsoft 11

APPENDIX A – CORE ONLINE SERVICES 13

APPENDIX B – SECURITY MEASURES 13

ONLINE SERVICE SPECIFIC TERMS 16

MICROSOFT AZURE SERVICES 16
MICROSOFT AZURE STACK 17
MICROSOFT COGNITIVE SERVICES 17
MICROSOFT GENOMICS 18
VISUAL STUDIO APP CENTER 18
MICROSOFT AZURE PLANS 19
AZURE ACTIVE DIRECTORY BASIC 19
AZURE ACTIVE DIRECTORY PREMIUM 19
AZURE INFORMATION PROTECTION PREMIUM 19
MICROSOFT DYNAMICS 365 SERVICES 19
OFFICE 365 SERVICES 21
EXCHANGE ONLINE 22
OFFICE 365 APPLICATIONS 23
MICROSOFT MYANALYTICS 24
OFFICE ONLINE 24
ONEDRIVE FOR BUSINESS 24
PROJECT ONLINE 24
SHAREPOINT ONLINE 25
SKYPE FOR BUSINESS ONLINE 25
OTHER ONLINE SERVICES 26
BING MAPS ENTERPRISE PLATFORM AND MOBILE ASSET MANAGEMENT PLATFORM 26
BUSINESS APPLICATION PLATFORM 27
MICROSOFT CLOUD APP SECURITY 27
MICROSOFT INTUNE 27
MICROSOFT KAIZALA PRO 28
MICROSOFT LEARNING 28
MINECRAFT: EDUCATION EDITION 28
OFFICE 365 DEVELOPER 28
WINDOWS DESKTOP OPERATING SYSTEM 29

ATTACHMENT 1 – NOTICES 30

BING MAPS 30
PROFESSIONAL SERVICES 30
NOTICE ABOUT AZURE MEDIA SERVICES H.265/HEVC ENCODING 32
NOTICE ABOUT ADOBE FLASH PLAYER 32
NOTICE ABOUT H.264/AVC VISUAL STANDARD, VC-1 VIDEO STANDARD, MPEG-4 PART 2 VISUAL STANDARD AND MPEG-2 VIDEO STANDARD 32

ATTACHMENT 2 – SUBSCRIPTION LICENSE SUITES 34

PUBLIC SECTOR 35

ATTACHMENT 3 – THE STANDARD CONTRACTUAL CLAUSES (PROCESSORS) 36

ATTACHMENT 4 – EUROPEAN UNION GENERAL DATA PROTECTION REGULATION TERMS 42

Introduction

The parties agree that these Online Services Terms govern Customer's use of the Online Services and set 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 and the processing and security of Support 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).

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
Microsoft Dynamics 365 Business Central Essentials	
Microsoft Dynamics 365 Business Central Premium	
Microsoft Dynamics 365 Business Central Team Member	

General

The OST has been restructured to improve clarity and organization. Definitions have been consolidated into a single standalone section entitled "Definitions." The General Terms have been reordered. And the data protection related terms previously spread across three separate sections—i.e., the Privacy and Security Terms, Data Processing Terms, and Appendix 1 to the GDPR Terms—have been consolidated into a single section entitled "Data Protection Terms."

Data Protection Terms

Location of Customer Data at Rest: Added France to the list of countries included in the Office 365 Services section to support the commencement of hosting services in datacenters located in France.
Appendix A – Core Online Services: Added Compliance Manager and Microsoft To-Do to the Office 365 Services section of the Core Online Services table.

Online Service Specific Terms

Microsoft Dynamics 365 Services: Added terms outlining the requirements for mixed deployments of Microsoft Dynamics 365 for Sales Professional and Microsoft Dynamics 365 for Sales Enterprise or Microsoft Dynamics 365 Business Central and Microsoft Dynamics 365 for Unified Operations.

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 in Appendix A to the Data Protection Terms.

"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 Support Data.

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

"General Data Protection Regulation" or "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.

"GDPR Terms" means the terms in Attachment 4, under which Microsoft makes binding commitments regarding its processing of Personal Data as required by Article 28 of the General Data Protection Regulation.

"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 the single physical hardware system to which a license is assigned. For purposes of this definition, a hardware partition or blade is considered to be a separate device.

"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.

"SL" means subscription license.

"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. The Standard Contractual Clauses are in Attachment 3.

"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.

The terms "data subject", "processing", "processor", and "supervisory authority" as used herein have the meanings given in the GDPR and the terms "data importer" and "data exporter" have the meanings given in the Standard Contractual Clauses.

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; or
- 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.

Violation of the terms 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.

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 data about the use and performance of the Apps, which may be transmitted to Microsoft and used for the purposes described in this OST for Customer Data.

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 www.microsoft.com/online/international-availability.aspx.

Compliance with Laws

Microsoft will comply with all laws and regulations applicable to its provision of the Online Services, including security breach notification law. 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 privacy, Personal Data, biometric data, data protection and confidentiality of communications. 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.

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).

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.

Data Protection Terms

This section of the Online Services Terms includes the following subsections:

- Scope
- Processing of Customer Data; Ownership
- Disclosure of Customer 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
- HIPAA Business Associate
- How to Contact Microsoft
- Appendix A – Core Online Services
- Appendix B – Security Measures

Scope

The terms in this section ("Data Protection Terms") apply to all Online Services except Bing Maps Enterprise Platform, Bing Maps Mobile Asset Management Platform, Bing Search Services, LinkedIn Sales Navigator, Microsoft Azure Stack, Microsoft Genomics, Microsoft Translator, and Visual Studio Mobile Center, 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, Previews are not included in the SLA for the corresponding Online Service, and 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 section ("Data Protection Terms") do not apply to Previews: Processing of Personal Data; GDPR, Data Security, and HIPAA Business Associate.

Attachment 1 includes the terms that apply to Professional Services, including privacy and security of Support Data and Personal Data in connection with the provision of those services. Therefore, unless expressly made applicable in Attachment 1, the terms in this section ("Data Protection Terms") do not apply to the provision of Professional Services.

Processing of Customer Data; Ownership

Customer Data will be used or otherwise processed only to provide Customer the Online Services including purposes compatible with providing those services. Microsoft will not use or otherwise process Customer Data or derive information from it for any advertising or similar commercial purposes. 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 to provide the Online Services to Customer. This paragraph does not affect Microsoft's rights in software or services Microsoft licenses to Customer.

Disclosure of Customer Data

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

Microsoft will not disclose Customer Data to law enforcement unless required by law. If law enforcement contacts Microsoft with a demand for Customer Data, Microsoft will attempt to redirect the law enforcement agency to request that data directly from Customer. If compelled to disclose Customer 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 Customer 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 Customer Data; (b) platform encryption keys used to secure Customer Data or the ability to break such encryption; or (c) access to Customer 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

Personal Data provided to Microsoft by, or on behalf of, Customer through use of the Online Service is also Customer Data. Pseudonymized identifiers may also be generated through Customer's use of the Online Services and are also Personal Data. To the extent Microsoft is a processor or subprocessor of Personal Data subject to the GDPR, the GDPR Terms in Attachment 4 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 when (a) Customer acts as a processor of Personal Data, in which case Microsoft is a subprocessor or (b) stated otherwise in the Online Service-specific terms. Microsoft will process Personal Data only on documented instructions from Customer. Customer agrees that its volume licensing agreement (including the OST) along with 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. 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.

Processing Details

The parties acknowledge and agree that:

- The subject-matter of the processing is limited to Personal Data within the scope of the GDPR;
- The duration of the processing shall be for the duration of the Customer's right to use the Online Service and until all Personal Data is deleted or returned in accordance with Customer instructions or the terms of the OST;
- The nature and purpose of the processing shall be to provide the Online Service pursuant to Customer's volume licensing agreement;
- The types of Personal Data processed by the Online Service include those expressly identified in Article 4 of the GDPR; and
- The categories of data subjects are Customer's representatives and end users, such as employees, contractors, collaborators, and customers.

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 Personal Data of data subjects and the ability to fulfill data subject requests to exercise their rights under the GDPR. Microsoft shall comply with reasonable requests by Customer to assist with Customer's response to such a data subject request. 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

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

Data Security

Security Practices and Policies

Microsoft will implement and maintain appropriate technical and organizational measures to protect Customer Data and Personal Data. 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 below and implements and maintains the security measures set forth in Appendix B 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 Business Application Platform Core Services	Yes	Yes

**Does not include Microsoft Dynamics 365 for Marketing, Microsoft Dynamics 365 for Sales Professional, Microsoft Social Engagement, Microsoft Dynamics 365 for Talent, Microsoft Dynamics 365 for Talent: Attract, and Microsoft Dynamics 365 for Talent: Onboard.*
***Current scope is detailed in the audit report and summarized in the Microsoft Azure Trust Center.*

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 above, 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 meets Customer's requirements, including any of its security obligations under the GDPR or other applicable data protection laws and regulations. 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.

If Customer has entered into the Standard Contractual Clauses with Microsoft or if the GDPR Terms apply, then Customer agrees to exercise its audit right by instructing Microsoft to execute the audit as described in this section of the OST. If Customer desires to change this instruction, then Customer has the right to do so as set forth in the Standard Contractual Clauses and GDPR Terms, which change shall be requested in writing.

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 OST 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 GDPR. 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 obligation to report or respond 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 OST, 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 in the event that it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Privacy Shield principles.

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 follows:

- **Office 365 Services.** If Customer provisions its tenant in Australia, Canada, the European Union, France, India, Japan, South Korea, the United Kingdom, 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, (3) files uploaded to OneDrive for Business, and (4) project content uploaded to Project Online.
- **Microsoft Intune Online Services**. When Customer provisions a tenant account, Customer selects an available Geo where Customer Data at rest will be stored. Microsoft will not transfer the Customer Data outside of Customer's selected Geo except as noted in the "Data Location" section of the Microsoft Intune Trust Center.
- **Microsoft Business Application Platform Core Services**. If Customer provisions its tenant in Australia, Canada, Asia Pacific, India, Japan, the European Union, United Kingdom (Power BI only), 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 Business Application 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, as detailed in the Microsoft Azure Trust Center (which Microsoft may update from time to time, but Microsoft will not add exceptions for existing Services in general release).
- **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.
- **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 (which Microsoft may update from time to time).

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 to retain such data or authorized in this agreement.

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, and (ii) will be obligated to maintain the confidentiality and security of such data even after their engagement ends.

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 Subprocessor's compliance with Microsoft's obligations in the OST. 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 OST.

From time to time, Microsoft may engage new Subprocessors. Microsoft will give Customer notice (by updating the website and provide 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 Customer Data or Personal Data. However, with respect to Core Online Services, Microsoft will give Customer notice (by updating the website and provide 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.

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 that includes an explanation of the grounds for non-approval. 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 OST, 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.

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;
- if Customer has multiple volume licensing agreements, the volume licensing agreement to which the opt out applies.

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

Table of Contents / General Terms

Appendix A – 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: Microsoft Dynamics 365 for Customer Service, Microsoft Dynamics 365 for Field Service, Microsoft Dynamics 365 Business Central, Microsoft Dynamics 365 for Finance and Operations, Enterprise edition, Microsoft Dynamics 365 for Marketing, Microsoft Dynamics 365 for Project Service Automation, Microsoft Dynamics 365 for Retail, Microsoft Dynamics 365 for Talent, Microsoft Dynamics 365 for Talent: Attract, Microsoft Dynamics 365 for Talent: Onboard, Microsoft Dynamics 365 for Sales, Microsoft Dynamics 365 for Sales Professional, and Microsoft Social Engagement. Microsoft Dynamics 365 Core Services do not include (1) Microsoft Dynamics 365 Services for supported devices or software, which includes but is not limited to Microsoft 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 Microsoft 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 MyAnalytics, Microsoft Planner, Microsoft StaffHub, Microsoft Teams, Microsoft To-Do, Office 365 Advanced Threat Protection, Office 365 Video, Office Online, OneDrive for Business, Outlook Customer Manager, Project Online, SharePoint Online, Skype for Business Online, Sway, and Yammer Enterprise. 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 Container Service, Azure Cosmos DB (formerly DocumentDB), Azure DevTest Labs, Azure DNS, Azure Information Protection (including Azure Rights Management), Azure Resource Manager, Backup, Batch, BizTalk Services, Cloud Services, Data Catalog, Data Factory, Data Lake Analytics, Data Lake Store, Event Hubs, Express Route, 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, Redis Cache, Scheduler, Security Center, Service Bus, Service Fabric, Site Recovery, SQL Data Warehouse, SQL Database, SQL Server Stretch Database, Storage, StorSimple, Stream Analytics, Traffic Manager, Virtual Machines, Virtual Machine Scale Sets, Virtual Network, Visual Studio Team Services, 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 Business Application 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 PowerApps, and Microsoft Flow. Microsoft Business Application Platform Core Services do not include any client software, including but not limited to Power BI Report Server, the Power BI, PowerApps or Microsoft Flow mobile applications, Power BI Desktop, or PowerApps Studio.

Appendix B – 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 the OST (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.

Domain	Practices
	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** - 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.

Domain	Practices
	- 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.
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

Online Service Specific Terms

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, Entity Search, Image Search, News Search, Video Search, Web Search, Spell Check, and Autosuggest APIs, and any other APIs identified at https://aka.ms/r1j7jq.

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

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

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 Non-Microsoft Products 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.

Microsoft Azure Stack
Microsoft Azure Stack is a Microsoft Azure Service.

Microsoft Azure Stack Privacy
The Enterprise and Developer Privacy Statement located at https://www.microsoft.com/en-us/privacystatement/EnterpriseDev applies to Customer's use of Microsoft Azure Stack. If a Microsoft Cloud Agreement Customer uses Microsoft Azure Stack 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.

Use of Microsoft Azure Stack
Customer may use Microsoft Azure Stack only on the hardware on which it is preinstalled. Microsoft Azure Stack includes Windows Server, Windows Software Components and SQL Server Technology, each of which are subject to the Included Technologies section of the Product Terms and may not be used outside of Microsoft Azure Stack.

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

Table of Contents / General Terms

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

Use of Specified Cognitive Services Data
Customer is solely responsible for the content of all Specified Cognitive Services Data.

Microsoft may process Specified Cognitive 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, Specified Cognitive 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 Specified Cognitive 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.

Where Specified Cognitive Services Data includes Personal Data, Customer will obtain sufficient consent for such processing by Microsoft from the data subjects (or from their parents or guardians as required by applicable law).

Microsoft is committed to helping protect data subjects who may be identifiable from Specified Cognitive Services Data that Microsoft retains. Microsoft has implemented business and technical measures designed to help de-identify some retained Specified Cognitive Services Data.

This Use of Specified Cognitive 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 Specified Cognitive Services Data. Microsoft acquires no rights in Specified Cognitive Services Data, other than the rights Customer grants to Microsoft in this Use of Specified Cognitive Services Data section. This paragraph does not affect Microsoft's rights in software or services Microsoft licenses to Customer.

Data Retention
Bing Search Services and Microsoft Translator are not designed to store Customer Data on Customer's behalf.

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

Bing Search Services and Microsoft Translator Limit on Customer use of service output:
Customer may not use any data from the Bing Search Services or Microsoft Translator for the purpose of developing or offering any comparable machine-learning based 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.

Precedence:
This Microsoft Cognitive Services section controls to the extent there is any conflict with other parts of the OST.

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").

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/mctestprivacypolicy 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. Microsoft will only use such data to provide Customer the Visual Studio App Center service, including purposes compatible with providing the service.

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.

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

Microsoft Dynamics 365 for Case Management, Enterprise edition
Microsoft Dynamics 365 for Customer Service, Enterprise edition
Microsoft Dynamics 365 for Field Services, Enterprise edition
Microsoft Dynamics 365 Business Central Essentials
Microsoft Dynamics 365 Business Central Premium
Microsoft Dynamics 365 Business Central Team Member
Microsoft Dynamics 365 for Marketing
Microsoft Dynamics 365 for Operations Activity, Enterprise edition
Microsoft Dynamics 365 for Operations Device, Enterprise edition
Microsoft Dynamics 365 for Project Service Automation, Enterprise edition
Microsoft Dynamics 365 for Retail, Enterprise edition
Microsoft Dynamics 365 for Sales, Enterprise edition
Microsoft Dynamics 365 for Sales Professional
Microsoft Dynamics 365 for Talent, Enterprise edition
Microsoft Dynamics 365 for Talent: Attract, Enterprise edition
Microsoft Dynamics 365 for Talent: Onboard, Enterprise edition
Microsoft Dynamics 365 for Team Members, Business edition
Microsoft Dynamics 365 for Team Members, Enterprise edition
Microsoft Relationship Sales solution

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

Subscription License Suites
In addition to User SLs, refer to Attachment 2 for other offerings that fulfill SL requirements.

External Users
External Users of Microsoft 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 Microsoft Dynamics 365 client software with Microsoft Dynamics 365 Services other than services or components included in the Microsoft Dynamics 365 Unified Operations Plan, Microsoft Dynamics 365 for Retail, Microsoft Dynamics 365 for Talent, Microsoft Dynamics 365 for Talent: Attract, or Microsoft Dynamics 365 for Talent: Onboard.

Administration Portal
Microsoft Dynamics 365 for Finance and Operations, Microsoft Dynamics 365 for Retail, and Microsoft Dynamics 365 for Talent enable Customers to deploy and manage the Online Service through Microsoft Dynamics Lifecycle Services (or its successor), which is subject to separate terms.

Mixed deployments of Microsoft Dynamics 365 services
Customers who wish to mix (i) Microsoft Dynamics 365 for Sales Professional and Microsoft Dynamics 365 for Sales Enterprise or (ii) Microsoft Dynamics 365 Business Central and Microsoft Dynamics 365 for Unified Operations may do so if:

- Each Online Service is deployed under a separate instance,
- All users accessing the instance are licensed with the single choice of Online Service, and
- No users have direct or indirect access to instances deployed with the other Online Service

Microsoft Dynamics 365 for Marketing
Service Level Agreement
There is no SLA for Microsoft Dynamics 365 for 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.

Microsoft Dynamics 365 Unified Operations Plan
Customer may modify for its internal use the application source code for Microsoft Dynamics 365 Finance and Operations and Microsoft Dynamics 365 for Retail

Microsoft Dynamics 365 for Talent, Microsoft Dynamics 365 for Talent: Attract, and Microsoft Dynamics 365 Talent: Onboard
Users accessing the Online Service who are (1) candidates in the attract module or (2) new hires in the onboard module do not need a SL.

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 Microsoft Dynamics 365 for Sales Professional, Microsoft Dynamics 365 for Marketing, Microsoft Dynamics 365 Business Central, Microsoft Dynamics 365 for Talent: Attract, Microsoft Dynamics 365 for Talent: Onboard, or Customers licensed for Dynamics 365 online services in Open License, Open Value and Open Value Subscription.

Microsoft Dynamics 365 for Operations On-premises Server
Customer's with active subscriptions for (1) Microsoft Dynamics 365 Plan or (2) Microsoft Dynamics 365 Unified Operations Plan (or any separately licensed component of the Plan) may:

- install any number of copies of the Microsoft Dynamics 365 for Operations Server software on a network server or shared servers;
- install and use Microsoft Dynamics AX 2012 R3 Server software in lieu of Microsoft Dynamic 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.

Microsoft Dynamics 365 On-premises Server
Customer with active subscriptions for (1) Microsoft Dynamics 365 Plan or (2) Microsoft Dynamics 365 Customer Engagement Plan (or any separately licensed component of the Plan) may:

- install any number of copies of Microsoft Dynamics 365 server (on-premises) software on a network server or shared servers;
- install Microsoft Dynamics CRM 2016 Server software in lieu of Microsoft Dynamic 365 On-Premise Server;
- allow access to the server software 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: Microsoft Dynamics 365 On-premises for Sales, Customer Service or Team Members CALs; or Microsoft Dynamics CRM CAL. Users and devices assigned CALs with active Software Assurance may access new versions of the server software.

Microsoft Relationship Sales solution

Microsoft Relationship Sales solution includes Microsoft Dynamics 365 for Sales, Enterprise edition and LinkedIn Sales Navigator, Enterprise edition. LinkedIn Sales Navigator, Enterprise edition 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. 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), 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 importer) and Customer (as data exporter) will comply with the applicable standard contractual clauses located at: https://business.linkedin.com/c/15/10/eu-scc.

Service Level Agreement

There is no SLA for LinkedIn Sales Navigator, Enterprise Edition.

Microsoft Social Engagement

Service Level Agreement

There is no SLA for Microsoft Social Engagement.

Social Content Obtained through Microsoft Social Engagement

Social Content is publicly-available content collected from social media networks (such as Twitter, Facebook and YouTube) and data indexing or data aggregation services in response to Customer's search queries executed in Microsoft Social Engagement. Social Content is not Customer Data. Customer Data used in configuring or initiating search queries executed on Customer's behalf may be shared with third parties for purposes of collecting Social Content. Customer may use Social Content for its internal business purposes only. Microsoft reserves the right to:

- store Social Content in a database commingled with content aggregated from other sources by other licensees;
- access, edit or delete Social Content in response to a request from a social media network, data indexing or data aggregation service, Social Content owner or a takedown request under the Digital Millennium Copyright Act;
- instruct Customer to edit or delete Social Content if Customer exports Social Content; and delete or restrict further access to Social Content after the Online Service has been terminated or expires.

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.

Subscription License Suites
In addition to User SLs, refer to Attachment 2 for other SLs that fulfill requirements for Office 365 Services.

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

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

Exchange Online

Office 365 Advanced Threat Protection
Office 365 Threat Intelligence
Data Loss Prevention
Exchange Online Archiving for Exchange Online
Exchange Online Archiving for Exchange Server
Exchange Online F1
Exchange Online (Plan 1 and Plan 2)

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 non-shared 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.

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.

Data Loss Prevention Device License
If Customer is licensed for 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 or Office 365 Threat Intelligence.

Table of Contents / General Terms

Office 365 Applications

Office 365 Business
Office 365 ProPlus
Visio Online (Plan 1 and Plan 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, and use shared computer activation, on a shared device, a network server, or on shared servers on Microsoft Azure or with a Qualified Multitenant Hosting Partner. A list of Qualified Multitenant Hosting Partners and additional deployment requirements are available at www.office.com/sca. For the purpose of this use right "network server" means a physical hardware server solely dedicated to Customer use. This shared computer activation provision does not apply to Customers licensed for Office 365 Business; 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.
- may use Internet-connected Online Services provided as part of ProPlus. 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 following terms apply only to Office 365 Business and Office 365 ProPlus

Smartphone and Tablet Devices
Each user to whom Customer assigns a User SL may also activate Microsoft Office Mobile software to use on up to five smartphones and five tablets.

The following terms apply only to Office 365 ProPlus

Office Home & Student 2013 RT Commercial Use

Each User SL for Office 365 ProPlus modifies the user's right to use the software under a separately acquired Office Home & Student 2013 RT license by waiving the prohibition against commercial use. Except for this allowance for commercial use of the software, all use is subject to the terms and use rights provided with the Office Home & Student 2013 RT License.

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. 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 or other Microsoft agreement that cover Online Services only.

Subscription License Suites

In addition to Office 365 ProPlus User SLs, Customer may fulfill the SL requirement for this Product by purchasing a Suite SL (refer Attachment 2).

Table of Contents / General Terms

Microsoft MyAnalytics

Service Level Agreement

There is no SLA for Microsoft MyAnalytics.

Table of Contents / General Terms

Office Online

Core Features for Office 365 Services

Office Online 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 Online or its successor service.

External Users

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

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 Online

Project Online Essentials
Project Online Professional
Project Online Premium

Installation and Use Rights for Project application

Each user to whom Customer assigns a Project Online Professional or Project Online Premium 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 shared servers with a qualified cloud partner. A list of qualified cloud partners and additional deployment requirements is available at www.office.com/sca. For the purpose of this use right "network server" means a physical hardware server solely dedicated to Customer use; 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.

Table of Contents / General Terms

SharePoint Online

Duet Enterprise Online for Microsoft SharePoint and SAP	SharePoint Online (Plan 1 and Plan 2)
SharePoint Online F1	

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 F1, 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

Skype for Business Online

Skype for Business Online (Plan 1 and Plan 2)	Common Area Phone
Audio Conferencing	Communication Credits
Calling Plan	Phone System

Notices

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

Core Features for Office 365 Services

Skype for Business Online Plan 1 and 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.

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 Phones

A Common Area Phone is a device that makes and receives only voice calls and is shared by multiple users who do not log into the device with their Office 365 credentials. Microsoft's Common Area Phone offering is a Device SL. Each Common Area Phone 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 enable users to communicate with others via the worldwide voice telephone network known generally as the Public Switched Telephone Network. Calling and Conferencing services are provided by the Microsoft Affiliate authorized to provide them. Pricing for Calling and Conferencing services may include applicable taxes and fees. The terms of use for Calling and Conferencing services may vary from country to country. All included taxes, fees and country-specific terms of use are disclosed on the Volume Licensing site (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

Other Online Services

Bing Maps Enterprise Platform and Mobile Asset Management Platform

Service SLs
A Service SL is required to access the services via the Bing Maps Enterprise Platform or Mobile Asset Management Platform. Each Service SL must be purchased with at least one of the following qualifying Add-On SLs:

- For the Bing Maps Enterprise Platform Service SL, either:
  - Bing Maps Public Website Usage Add-on SL, which is available for a specified number of billable transactions for use on a website that is available publicly without restriction,
  - Bing Maps Internal Website Usage Add-on SL, which is available for a specified number of billable transactions for use on an internal website (e.g., intranet) on a private network,
  - Bing Maps Known User Add-on SL, or
  - Bing Maps Light Known User Add-on SL.
- For the Mobile Asset Management Platform Service SL; for each Asset either:
  - 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)

Qualifying Mobile Asset Management Platform Service SL Add-on SLs
For the Mobile Asset Management Platform, an Add-on SL is required for each tracked Asset whose GPS or other sensor based position can be monitored, displayed, reverse geocoded or used to perform calculations using Mobile Asset Management Platform. "Asset" is defined as any vehicle, device or other mobile object. These Add-on SLs are for a specified number of tracked Assets.

Authenticated Users
Users that are authenticated by Customer's programs that access Bing Maps Enterprise Platform and Mobile Asset Management Platform must have a SL.

Bing Maps APIs
Customer may use all Bing Maps APIs in accordance with the Microsoft Bing Maps Platform API Terms of Use and Bing Maps Platform SDKs, including any successors thereto, located at https://aka.ms/bingmapsplatformapistou and https://aka.ms/bingmapsplatformsdks/.

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

Table of Contents / General Terms

Business Application Platform

Microsoft Flow
Microsoft PowerApps
Microsoft Power BI Pro
Microsoft Power BI Premium
Microsoft Stream

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.

Table of Contents / General Terms

Microsoft Cloud App Security

Notices

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

Table of Contents / General Terms

Microsoft Intune

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

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. Each device to which customer assigns an SL may access and use the Online Services and related software (including System Center software) for use by any number of users. Management of a device accessed by more than one user requires a Device SL or a User SL for each user.

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, Microsoft 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 unified installer of the software. Customer must obtain Microsoft's prior written approval to disclose to a third party the results of any benchmark test of these components or the software that includes them.

Table of Contents / General Terms

Microsoft Kaizala Pro

Service Level Agreement
There is no SLA for Microsoft Kaizala Pro.

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

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

Windows Desktop Operating System

Data Retention

The Windows Defender Advanced Threat Protection and Windows Analytics portion of the product does not contain extractable Customer Data therefore the Customer Data extraction terms in the OST do not apply.

Table of Contents / General Terms

Attachment 1 – Notices

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 Bing Maps 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 included in a separate agreement, then the terms of that separate agreement will apply.

The Professional Services to which this Notice applies are not Online Services, and the rest of the Online Services Terms, as well as any data processing amendment or HIPAA Business Associated Agreement signed by the parties, do not apply unless expressly made applicable by the Professional Services Terms below.

Support Data

Processing of Support Data

Support Data will be used and otherwise processed only to provide Customer with technical support, including purposes compatible with providing technical support. Microsoft will not use or otherwise process Support Data or derive information from it for advertising or similar commercial purposes without Customer's permission. As between the parties, Customer retains all right, title and interest in and to Support Data. Microsoft acquires no rights in Support Data, other than the rights Customer grants to Microsoft to provide support to Customer. This paragraph does not affect Microsoft's rights in software or services Microsoft licenses to Customer.

Processing of Personal Data included in Support Data; GDPR

Personal Data provided to Microsoft by, or on behalf of, Customer in connection with the provision of technical support is also Support Data. To the extent Microsoft is a processor or subprocessor of Personal Data subject to the GDPR, the GDPR Terms in Attachment 4 govern that processing and the parties also agree to the following terms in this sub-section ("Processing of Personal Data included in Support Data; GDPR"):

Processor and Controller Roles and Responsibilities

Customer and Microsoft agree that Customer is the controller of Personal Data included in Support 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. However, Microsoft and Customer agree that Microsoft is the data controller for business contact information or other Personal Data that may be collected at the same time as Support Data but is needed to maintain the business relationship with the Customer. Microsoft will process Personal Data only on documented instructions from Customer. Customer agrees that its volume licensing agreement (including the OST) along with Customer's use of Professional Services are Customer's complete and final documented instructions to Microsoft for the processing of Personal Data. 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.

Processing of Personal Data included in Support Data

The parties acknowledge and agree that:

- The subject-matter of the processing is limited to Personal Data within the scope of the GDPR;
- The duration of the processing shall be for the duration of the Customer's right to receive technical support and until all Personal Data is deleted or returned in accordance with Customer instructions or the terms of the OST;
- The nature and purpose of the processing shall be to provide technical support pursuant to Customer's volume licensing agreement;
- The types of Personal Data processed in connection with the provision of technical support include those expressly identified in Article 4 of the GDPR; and
- The categories of data subjects are Customer's representatives and end users, such as employees, contractors, collaborators, and customers.

For data subject requests and records of processing activities related to Support Data, and Personal Data included therein, Microsoft will abide by the applicable obligations set forth in the "Data Subject Rights; Assistance with Requests" and "Records of Processing Activities" provisions in the Data Protection Terms section of the OST.

Security of Support Data

Microsoft will implement and maintain technical and organizational measures to protect Support Data. If Microsoft becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Support Data while processed by Microsoft, Microsoft will abide by the obligations set forth in the "Security Incident Notification" provision in the Data Protection Terms section of the OST.

Data Location and Transfer

Support Data that Microsoft processes on Customer's behalf may be transferred to, and stored and processed in, the United States or any other country in which Microsoft or its Affiliates or Subprocessors operate. Customer appoints Microsoft to perform any such transfer of Support Data to any such country and to store and process that data to provide technical support. Microsoft is certified to the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks and the commitments they entail. Microsoft agrees to notify Customer in the event that it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Privacy Shield principles.

Other Support Data Commitments

Disclosure

The disclosure of Support Data by Microsoft to third parties is governed by the same restrictions and procedures that govern Customer Data set forth in the "Disclosure of Customer Data" provision in the Data Protection Terms section of the OST.

Deletion or Return

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

Use of Subprocessors

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 "Use of Subprocessors" provision in the Data Protections Terms section of the OST.

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 OST also apply with respect to Support Data.

Other Professional Services Terms

Processing of Personal Data

To the extent Microsoft is a processor or subprocessor of Personal Data, not included within Support Data, in connection with the provision of Professional Services, Microsoft makes the commitments in the GDPR Terms in Attachment 4 to all customers effective May 25, 2018.

Obligations of the Parties

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.

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.

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. **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. No limitation or exclusions will apply to liability arising out of either party's (1) confidentiality obligations; 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.

Services Deliverables
"Services Deliverables" means any computer code or materials other than Products or Fixes that Microsoft leaves with Customer at the conclusion of Microsoft's performance of Professional Services. Microsoft grants Customer a non-exclusive, non-transferable, perpetual license to reproduce, use, and modify the Services Deliverables solely for Customer's internal business purposes, subject to the terms and conditions in Customer's volume licensing agreement.

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.

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 [2]			Microsoft 365 Business	Dynamics 365 Enterprise Edition		
	F1	E1	E3	E5			E3	E5	F1	E3	E5		Cust Eng[4]	Uni Ops[4]	Plan
Exchange Online					■										
Exchange Online K1	■								■						
Exchange Online Plan 1		■				■						■			
Exchange Online Plan 2			■	■						■	■				
SharePoint Online					■										
SharePoint Online K1	■								■						
SharePoint Online Plan 1		■				■						■			
SharePoint Online Plan 2			■	■						■	■				
Skype for Business Online Plan 1	■				■				■						
Skype for Business Online Plan 2		■	■	■		■				■	■	■			
Phone System				■							■				
Audio Conferencing				■							■				
Office Online	■	■	■	■	■	■			■	■	■	■			
Office 365 Business						■						■			
Office 365 ProPlus			■	■						■	■				
Microsoft MyAnalytics				■							■				
Office 365 Advanced Compliance				■							■				
Office 365 Cloud App Security				■							■				
Office 365 Threat Intelligence				■							■				
Microsoft Power BI Pro				■							■				
Office 365 Advanced Threat Protection				■							■				
Microsoft Intune							■	■	■	■	■				
Azure Info Protection Premium Plan 1							■			■					
Azure Info Protection Premium Plan 2								■			■				
Azure Active Directory Premium Plan 1							■		■	■					
Azure Active Directory Premium Plan 2								■			■				
Azure Advanced Threat Protection for Users								■			■				
Microsoft Cloud App Security								■			■				
Microsoft Dynamics 365 for Customer Service													■		■
Microsoft Dynamics 365 for Field Service													■		■
Microsoft Dynamics 365 for Project Service Automation													■		■
Microsoft Dynamics 365 for Retail														■	■
Microsoft Dynamics 365 for Sales Enterprise													■		■
Microsoft Dynamics 365 for Talent														■	■
Microsoft Flow Plan 1												■		■	■
Microsoft PowerApps Plan 1														■	■
Microsoft PowerApps Plan 2													■	■	■
Microsoft Stream Plan 1		■	■							■					
Microsoft Stream Plan 2				■							■				

[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 Enterprise E5 is dependent on regional availability.
[4] In addition to the Online Services identified above, Dynamics 365 Unified Operations Plan includes finance and operations functionality as described in Appendix C of the Dynamics 365 Enterprise edition Licensing Guide https://www.microsoft.com/en-us/dynamics365/pricing.

Public Sector

Online Service	Office 365 Government[1,3]					Office 365 Education[3]			Microsoft 365 Education[2]		
	F1	E1	E3	E4	E5	A1	A3	A5	A1	A3[5]	A5
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 1	■										
Skype for Business Online Plan 2		■	■	■	■	■	■	■		■	■
Phone System					■		■	■			■
Audio Conferencing					■		■	■			■
Office Online	■	■	■	■	■	■	■	■	■	■	■
Office 365 ProPlus			■	■	■		■	■		■	■
Microsoft MyAnalytics					■			■			■
Office 365 Advanced Compliance					■			■			■
Office 365 Cloud App Security					■		■	■		■	■
Office 365 Threat Intelligence					■			■			■
Microsoft Power BI Pro					■			■			■
Office 365 Advanced Threat Protection					■			■			■
Microsoft Intune									■		
Azure Info Protection Premium Plan 1										■	
Azure Info Protection Premium Plan 2											■
Azure Active Directory Premium Plan 1										■	
Azure Active Directory Premium Plan 2											■
Azure Advanced Threat Protection for Users											■
Microsoft Cloud App Security											■
Microsoft Stream Plan 1		■	■	■		■	■			■	
Microsoft Stream Plan 2					■			■			■
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 Government/Education E5/A5 is dependent on regional availability.
[5]Includes Microsoft 365 Education A3 with Core CAL.

Table of Contents / General Terms

Attachment 3 – The Standard Contractual Clauses (Processors)

Execution of the volume licensing agreement by Customer includes execution of this Attachment 3, 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 section of the OST entitled “Data Protection Terms.”

Data importer: The data importer is MICROSOFT CORPORATION, a global producer of software and services.

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

Categories of data: The personal data transferred includes e-mail, documents and other data in an electronic form in the context of the Online Services.

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

a. Duration and Object of Data Processing. The duration of data processing shall be for the term designated under the applicable volume licensing agreement between 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 Security Practices and Policies section of the OST. 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.

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 applicable to the agreement.

Subcontractors: 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):

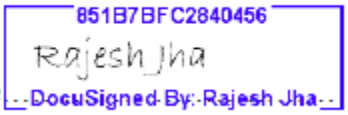
1. **Personnel**. Data importer's personnel will not process Customer Data without authorization. Personnel are obligated to maintain the confidentiality of any Customer Data and this obligation continues even after their engagement ends.

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 OST, 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 OST 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 

Rajesh Jha, Corporate Vice President
Microsoft Corporation
One Microsoft Way, Redmond WA, USA 98052

Attachment 4 – 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 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.