

Volume
Licensing

Online Services Terms January 1, 2015

Table of Contents

INTRODUCTION	3	ONEDRIVE FOR BUSINESS.....	20
PRIOR VERSIONS	3	PROJECT ONLINE.....	20
CLARIFICATIONS AND SUMMARY OF CHANGES.....	3	SHAREPOINT ONLINE.....	20
GENERAL TERMS	4	OTHER ONLINE SERVICES.....	21
Definitions.....	4	BING MAPS ENTERPRISE PLATFORM AND BING MAPS MOBILE ASSET	
Online Service Term Updates.....	4	MANAGEMENT PLATFORM.....	21
Regulatory Changes & International Availability	4	MICROSOFT LEARNING E-REFERENCE LIBRARY	21
Data Retention	4	MICROSOFT LEARNING IT ACADEMY	21
Use of Software with the Online Service	4	OFFICE 365 DEVELOPER.....	22
Non-Microsoft Products.....	5	POWER BI FOR OFFICE 365	22
Acceptable Use Policy	5	SYSTEM CENTER ENDPOINT PROTECTION.....	22
Technical Limitations	5	TRANSLATOR API.....	22
Compliance with Laws.....	5	YAMMER ENTERPRISE.....	22
Electronic Notices	5	ATTACHMENT 1 – NOTICES.....	24
License Reassignment	6	BING MAPS.....	24
Font Components.....	6	CUSTOMER SUPPORT.....	24
Multiplexing.....	6	NOTICE ABOUT H.264/AVC VISUAL STANDARD, VC-1 VIDEO STANDARD,	
PRIVACY AND SECURITY TERMS	7	MPEG-4 PART VISUAL STANDARD AND MPEG-2 VIDEO STANDARD	25
GENERAL PRIVACY AND SECURITY TERMS	7	ATTACHMENT 2 – SUBSCRIPTION LICENSE SUITES	26
Scope.....	7	ATTACHMENT 3 – THE STANDARD CONTRACTUAL CLAUSES	
Use of Customer Data	7	(PROCESSORS).....	27
Disclosure of Customer Data.....	7		
Educational Institutions	7		
Security	7		
Security Incident Notification	8		
Location of Data Processing.....	8		
Preview Releases.....	8		
Use of Subcontractors.....	8		
How to Contact Microsoft.....	8		
DATA PROCESSING TERMS	8		
Location of Customer Data at Rest	9		
Privacy.....	9		
Additional European Terms.....	10		
Security	10		
Certifications and Audits.....	12		
ONLINE SERVICE SPECIFIC TERMS	14		
MICROSOFT AZURE SERVICES	14		
ENTERPRISE MOBILITY SERVICES	15		
AZURE ACTIVE DIRECTORY BASIC.....	15		
AZURE ACTIVE DIRECTORY PREMIUM	15		
AZURE RIGHTS MANAGEMENT SERVICE	15		
AZURE REMOTEAPP	15		
MICROSOFT INTUNE.....	16		
MICROSOFT DYNAMICS ONLINE SERVICES	16		
MICROSOFT DYNAMICS CRM ONLINE	16		
MICROSOFT DYNAMICS MARKETING	16		
MICROSOFT SOCIAL LISTENING.....	17		
PARATURE, FROM MICROSOFT.....	17		
OFFICE 365 SERVICES	17		
EXCHANGE ONLINE.....	17		
LYNC ONLINE	19		
OFFICE 365 APPLICATIONS	19		
OFFICE ONLINE	20		

Introduction

Beginning July 1, 2014 these Online Services Terms (OST) replace the Online Services Use Rights (OLSUR). The OST contains terms that apply to Customer's use of Online Services. Separate terms, including different privacy and security terms, govern Customer's use of Non-Microsoft Products (as defined below), as well as other products and services from Microsoft.

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>.

Prior Versions

The OST provides terms for Online Services that are currently available. For earlier versions Customer may refer to <http://go.microsoft.com/?linkid=9840733> or contact its reseller or Microsoft Account Manager.

Clarifications and Summary of Changes

Enterprise Cloud Suite	
------------------------	--

Changes

General Terms

Clarified that free trials were excluded from Data Retention terms.
Removed Acquired Rights section.

Data Process Terms subsection of the Privacy and Security Terms

In the definition of "Online Services," revised definitions of Office 365 Services and Microsoft Intune Online Services.
In the Security subsection, clarified what is the Incident Response Process practice related to the Information Security Incident Management domain.

Lync Online

Clarified user SL requirements.

Microsoft Azure Services

Clarified that access to certain data centers may be restricted.

Microsoft Social Listening

Clarified that Social Content may only be used for internal business purposes.

Office 365 Applications

Replaced "SCA" with "shared computer activation."

Attachment 2, Subscription License Suites

Added Enterprise Cloud Suite.
Added Yammer Enterprise to Office 365 Enterprise K1 suite.
Added Enterprise Cloud Suite note.

General Terms

Customer may use the Online Services and related software as expressly permitted in Customer's volume licensing agreement. Microsoft reserves all other rights. Customer must acquire and assign the appropriate subscription licenses required for its use of each Online Service. A User SL is required for each user that accesses the Online Service 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.

Definitions

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

"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.

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

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

"Licensed Device" means 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.

"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 List. The Product List 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.

"SL" means subscription license.

Online Service Term Updates

When Customer renews or purchases a new subscription to an Online Service, the then-current OST 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 OST that apply to Customer's use of those new features, supplements or related software.

Regulatory Changes & International Availability

Microsoft may make commercially reasonable changes to each Online Service from time to time. Microsoft may terminate an Online Service in any country where Microsoft is subject to a government regulation, obligation or other requirement that is not generally applicable to businesses operating there. 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.

Data Retention

Except for free trials, Microsoft will retain Customer Data stored in the Online Service 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.

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

Use of Software with the Online Service

Customer may need to install certain Microsoft software in order 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.

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.

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). 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 the Non-Microsoft Product as part of Customer's bill for Online Services. Microsoft, however, assumes no responsibility or liability whatsoever for the Non-Microsoft Product. Customer is solely responsible for any Non-Microsoft Product that it installs or uses with an Online Service.

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.

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.

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, data protection and confidentiality of communications. 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), and for determining whether the Online Services are appropriate for storage and processing of information subject to any specific law or regulation. 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.

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.

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.

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.

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.

[Table of Contents](#)[Introduction](#)[General Terms](#)[Privacy and Security Terms](#)[Online Service – specific Terms](#)[Attachments](#)

Privacy and Security Terms

This section of the Online Services Terms has two parts:

- General Privacy and Security Terms, which apply to all Online Services; and
- Data Processing Terms, which are additional commitments for certain Online Services.

General Privacy and Security Terms

Scope

The terms in this section apply to all Online Services except Bing Maps Enterprise Platform, Bing Maps Mobile Asset Management Platform, Translator API, Yammer, and Parature, from Microsoft, which are governed by the privacy and/or security terms referenced below in the applicable [Online Service-specific Terms](#).

Use of Customer Data

Customer Data will be used only to provide Customer the Online Services including purposes compatible with providing those services. Microsoft will not use 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) with permission from an end user, (3) as described in the OST, or (4) as required by law.

Microsoft will not disclose Customer Data to law enforcement unless required by law. Should law enforcement contact 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, then 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 (such as requests from Customer's end users), Microsoft will promptly notify Customer unless prohibited by law. If Microsoft is not required by law to disclose the Customer Data, Microsoft will reject the request. If the request is valid and Microsoft could be compelled to disclose the requested information, Microsoft will attempt to redirect the third party to request the Customer Data from Customer.

Except as Customer directs, Microsoft will not provide any third party: (1) direct, indirect, blanket or unfettered access to Customer Data; (2) the platform encryption keys used to secure Customer Data or the ability to break such encryption; or (3) any kind of access to Customer Data if Microsoft is aware that such data is used for purposes other than those stated in the request.

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

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.

Security

Microsoft is committed to helping protect the security of Customer's information. Microsoft has implemented and will maintain and follow appropriate technical and organizational measures intended to protect Customer Data against accidental, unauthorized or unlawful access, disclosure, alteration, loss, or destruction.

Security Incident Notification

If Microsoft becomes aware of any unlawful access to any Customer Data stored on Microsoft's equipment or in Microsoft's facilities, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of Customer Data (each a "Security Incident"), Microsoft will promptly (1) notify Customer of the Security Incident; (2) investigate the Security Incident and provide Customer with detailed information about the Security Incident; and (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. 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.

Location of Data Processing

Except as described elsewhere in the OST, Customer Data that Microsoft processes on Customer's behalf may be transferred to, and stored and processed in, the United States or any other country in which Microsoft or its affiliates or subcontractors maintain facilities. Customer appoints Microsoft to perform any such transfer of Customer Data to any such country and to store and process Customer Data in order to provide the Online Services. Microsoft abides by the EU Safe Harbor and the Swiss Safe Harbor frameworks as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of data from the European Union, the European Economic Area, and Switzerland.

Preview Releases

Microsoft may offer preview, beta or other pre-release features and services ("Previews") for optional evaluation. Previews may employ lesser or different privacy and security measures than those typically present in the Online Services. Unless otherwise provided, Previews are not included in the SLA for the corresponding Online Service.

Use of Subcontractors

Microsoft may hire subcontractors to provide services on its behalf. Any such subcontractors will be permitted to obtain Customer Data only to deliver the services Microsoft has retained them to provide and will be prohibited from using Customer Data for any other purpose. Microsoft remains responsible for its subcontractors' compliance with Microsoft's obligations in the OST. Customer has previously consented to Microsoft's transfer of Customer Data to subcontractors as described in the OST.

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
Carmenhall Road
Sandyford, Dublin 18, Ireland

Data Processing Terms

The Data Processing Terms (DPT) include the terms in this section.

The Data Processing Terms also include the "Standard Contractual Clauses," pursuant to the European Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under the EU Data Protection Directive.

The Standard Contractual Clauses are in [Attachment 3](#). In addition,

- Execution of the volume licensing agreement includes execution of [Attachment 3](#), which is countersigned by Microsoft Corporation;

- The terms in Customer’s volume licensing agreement, including the DPT, constitute a data processing agreement under which Microsoft is the data processor; and
- The DPT control over any inconsistent or conflicting provision in Customer’s volume licensing agreement and, for each subscription, will remain in full force and effect until all of the related Customer Data is deleted from Microsoft’s systems in accordance with the DPT.

Customer may opt out of the “Standard Contractual Clauses” or the Data Processing Terms in their entirety. To opt out, 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;
- if opting out of the entire DPT, a statement that Customer (or Affiliate) opts out of the entirety of the Data Processing Terms; and
- if opting out of only the Standard Contractual Clauses, a statement that Customer (or Affiliate) opts out of the Standard Contractual Clauses only.

In countries where regulatory approval is required for use of the Standard Contractual Clauses, the Standard Contractual Clauses cannot be relied upon under European Commission 2010/87/EU (of February 2010) to legitimize export of data from the country, unless Customer has the required regulatory approval.

In the DPT, the term “Online Services” applies only to the services in the table below, excluding any Preview features or services, and “Customer Data” includes only Customer Data that is provided through use of those Online Services.

Microsoft Dynamics Online Services	Microsoft Dynamics Online services made available through volume licensing or the Microsoft online services portal, excluding (1) Microsoft Dynamics CRM for supported devices, which includes but is not limited to Microsoft Dynamics CRM Online services for tablets and/or smartphones and (2) any separately-branded service made available with or connected to Microsoft Dynamics CRM Online, such as Microsoft Social Listening, Parature, from Microsoft, and Microsoft Dynamics Marketing.
Office 365 Services	The following services, each as included in an Office 365-branded plan or suite: Exchange Online, Exchange Online Archiving, Exchange Online Protection, SharePoint Online, OneDrive for Business, Lync Online, and Office Online. Office 365 Services do not include Office 365 ProPlus or any separately branded service made available with an Office 365-branded plan or suite, such as a Bing or Yammer service or a service branded “for Office 365.”
Microsoft Azure Core Services	Cloud Services (web and worker roles), Virtual Machines (including with SQL Server), Storage (Blobs, Tables, Queues), Virtual Network, Traffic Manager, Web Sites, BizTalk Services, Media Services, Mobile Services, Service Bus, Multi-Factor Authentication, Active Directory, Rights Management Service, SQL Database, and any other features identified as included on the Microsoft Azure Trust Center.
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.

Location of Customer Data at Rest

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 the United States or the EU, Microsoft will store the following Customer Data at rest within that Geo: (1) Exchange Online mailbox content (e-mail body, calendar entries, and the content of e-mail attachments) and (2) SharePoint Online site content and the files stored within that site.
- **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 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 Dynamics CRM Online Services.** For entities managed by the Microsoft Dynamics CRM Online Service, if Customer provisions its tenant in the United States or EU, Microsoft will store Customer Data at rest in the United States or EU, as applicable.

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

Privacy

- **Customer Data Deletion or Return.** No more than 180 days after expiration or termination of Customer’s use of an Online Service, Microsoft will disable the account and delete Customer Data from the account.
- **Transfer of Customer Data.** Microsoft will, during the term designated under Customer’s volume licensing agreement, remain certified under the EU and Swiss Safe Harbor programs, provided that they are maintained by the United States government. In addition, unless Customer has opted out of the Standard Contractual Clauses, all transfers of Customer Data out of the European Union, European Economic Area, and Switzerland shall be governed by the Standard Contractual Clauses.
- **Microsoft Personnel.** Microsoft personnel will not process Customer Data without authorization from Customer. Microsoft personnel are obligated to maintain the security and secrecy of any Customer Data as provided in the DPT and this obligation continues even after their engagements end.
- **Subcontractor Transfer.** Any subcontractors to whom Microsoft transfers Customer Data, even those used for storage purposes, will have entered into written agreements with Microsoft that are no less protective than the DPT. Customer has previously consented to Microsoft’s transfer of Customer Data to subcontractors as described in the DPT. Except as set forth in the DPT, or as Customer may otherwise authorize, Microsoft will not transfer to any third party (not even for storage purposes) personal data Customer provides to Microsoft through the use of the Online Services. Each Online Service has a website that lists subcontractors that are authorized to access Customer Data. At least 14 days before authorizing any new subcontractor to access Customer Data, Microsoft will update the applicable website and provide Customer with a mechanism to obtain notice of that update. If Customer does not approve of a new subcontractor, then Customer may terminate the affected Online Service without penalty by providing, before the end of the 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 the terminated Online Services from subsequent Customer invoices.

Additional European Terms.

These Additional European Terms apply only if Customer has end users in the European Economic Area (“EEA”) or Switzerland.

- **End Users in EEA or Switzerland.** Terms used in the DPT that are not specifically defined will have the meaning in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the “EU Data Protection Directive”).
- **Intent of the Parties.** For the Online Services, Microsoft is a data processor (or sub-processor) acting on Customer’s behalf. As data processor (or sub-processor), Microsoft will only act upon Customer’s instructions. The OST and Customer’s volume licensing agreement (including the terms and conditions incorporated by reference therein) are Customer’s complete and final instructions to Microsoft for the processing of Customer Data. Any additional or alternate instructions must be agreed to according to the process for amending Customer’s volume licensing agreement.
- **Duration and Object of Data Processing.** The duration of data processing shall be for the term designated under Customer’s volume licensing agreement. The objective of the data processing is the performance of the Online Services.
- **Scope and Purpose of Data Processing.** The scope and purpose of processing of Customer Data, including any personal data included in the Customer Data, is described in the DPT and Customer’s volume licensing agreement.
- **Customer Data Access.** For the term designated under Customer’s volume licensing agreement Microsoft will, at its election and as necessary under applicable law implementing Article 12(b) of the EU Data Protection Directive, either: (1) provide Customer with the ability to correct, delete, or block Customer Data, or (2) make such corrections, deletions, or blockages on Customer’s behalf.

Security

- **General Practices.** Microsoft has implemented and will maintain and follow for the Online Services the following security measures, which, in conjunction with the security commitments in the OST, are Microsoft’s only responsibility with respect to the security of Customer Data.

<p>Organization of Information Security</p>	<p>Security Ownership. Microsoft has appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures.</p> <p>Security Roles and Responsibilities. Microsoft personnel with access to Customer Data are subject to confidentiality obligations.</p> <p>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.</p>
<p>Asset Management</p>	<p>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.</p> <p>Asset Handling</p> <ul style="list-style-type: none"> - Microsoft classifies Customer Data to help identify it and to allow for access to it to be appropriately

	<p>restricted.</p> <ul style="list-style-type: none"> - 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	<p>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.</p>
Physical and Environmental Security	<p>Physical Access to Facilities. Microsoft limits access to facilities where information systems that process Customer Data are located to identified authorized individuals.</p> <p>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.</p> <p>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.</p> <p>Component Disposal. Microsoft uses industry standard processes to delete Customer Data when it is no longer needed.</p>
Communications and Operations Management	<p>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.</p> <p>Data Recovery Procedures</p> <ul style="list-style-type: none"> - 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. - 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. <p>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.</p> <p>Data Beyond Boundaries</p> <ul style="list-style-type: none"> - 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 (e.g., through encryption). <p>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.</p>
Access Control	<p>Access Policy. Microsoft maintains a record of security privileges of individuals having access to Customer Data.</p> <p>Access Authorization</p> <ul style="list-style-type: none"> - 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. <p>Least Privilege</p> <ul style="list-style-type: none"> - 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. <p>Integrity and Confidentiality</p>

	<ul style="list-style-type: none"> - 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. <p>Authentication</p> <ul style="list-style-type: none"> - Microsoft uses industry standard practices to identify and authenticate users who attempt to access information systems. - Where authentication mechanisms are based on passwords, Microsoft requires that the passwords are renewed regularly. - Where authentication mechanisms are based on passwords, Microsoft requires the password to be at least eight characters long. - Microsoft ensures that de-activated or expired identifiers are not granted to other individuals. - Microsoft monitors, or enables Customer to monitor, repeated attempts to gain access to the information system using an invalid password. - Microsoft maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed. - Microsoft uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage. <p>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.</p>
<p>Information Security Incident Management</p>	<p>Incident Response Process</p> <ul style="list-style-type: none"> - 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 unreasonable delay and, in any event, within 30 calendar days. <p>Microsoft tracks, or enables Customer to track, disclosures of Customer Data, including what data has been disclosed, to whom, and at what time.</p> <p>Service Monitoring. Microsoft security personnel verify logs at least every six months to propose remediation efforts if necessary.</p>
<p>Business Continuity Management</p>	<ul style="list-style-type: none"> - 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.

Certifications and Audits

- Microsoft has established and agrees to maintain a data security policy (Online Information Security Policy) for each Online Service that complies with the ISO 27001 standards for the establishment, implementation, control, and improvement of the Information Security Management System and the ISO/IEC 27002 code of best practices for information security management. On a confidential need-to-know basis, and subject to Customer’s agreement to non-disclosure obligations Microsoft specifies, Microsoft will make the Online Information Security Policy available to Customer, along with other information reasonably requested by Customer regarding Microsoft security practices and policies. Customer is solely responsible for reviewing the Online Information Security Policy, making an independent determination as to whether the Online Information Security Policy meets Customer’s requirements, and for ensuring that Customer’s personnel and consultants follow the guidelines they are provided regarding data security. If Customer is subject to the Standard Contractual Clauses, then this section is in addition to Clause 5 paragraph f and Clause 12 paragraph 2 of the Standard Contractual Clauses.
- Microsoft will audit the security of the computers and computing environment that it uses in processing Customer Data (including personal data) on the Online Services and the physical data centers from which Microsoft provides the Online Services. This audit: (1) will be performed at least annually; (2) will be performed according to ISO 27001 standards; (3) will be performed by qualified, independent third party security professionals at Microsoft’s selection and expense; (4) will result in the generation of an audit report (Microsoft Audit Report), which will be Microsoft’s confidential information; and (5) may be performed for other purposes in addition to satisfying this section (e.g., as part of Microsoft’s regular internal security procedures or to satisfy other contractual obligations).
- If Customer requests in writing, Microsoft will provide Customer with a confidential summary of the Microsoft Audit Report (Summary Report) so that Customer can reasonably verify Microsoft’s compliance with the security obligations under the DPT. The Summary Report will clearly disclose the scope of the audit and any material findings by the auditor. The Summary Report is Microsoft confidential information.

- If the Standard Contractual Clauses apply, then Customer agrees to exercise its audit right by instructing Microsoft to execute the audit as described in this section of the DPT. If Customer has not opted out of the Standard Contractual Clauses and desires to change this instruction regarding exercising this audit right, then Customer has the right to change this instruction as mentioned in the Standard Contractual Clauses, which shall be requested in writing.
- If the Standard Contractual Clauses apply, then nothing in this section of the DPT varies or modifies the Standard Contractual Clauses nor affects any supervisory authority's or data subject's rights under the Standard Contractual Clauses. Microsoft Corporation is an intended third-party beneficiary of this section.

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Privacy and Security Terms](#)



[Online Service – specific Terms](#)



[Attachments](#)

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 Customer Support and 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 <http://azure.microsoft.com/en-us/support/legal/sla/>.

Definitions

“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.

“Managed Service Solution” means a managed IT service provided by Customer to a third party that consists of the administration of and support for Microsoft Azure Services.

“Microsoft Azure Services” means one or more of the Microsoft services and features identified at <http://azure.microsoft.com/en-us/services>, except where identified as licensed separately.

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.

Managed Service Exception

Customer may provide a Managed Service Solution provided (i) Customer has the sole ability to access, configure, and administer the Microsoft Azure Services, (ii) Customer has administrative access to the virtual OSE(s), if any, in the Managed Service Solution, and (iii) the third party has administrative access only to its application(s) or virtual OSE(s). Customer is responsible for the third party’s use of Microsoft Azure Services in accordance with the terms of the volume licensing agreement.

Virtual Machines

Microsoft Azure Services may provide Customer with the option of running Windows Server and other Microsoft software in a Virtual Machine. Customer agrees to secure the rights necessary to run all software (including the operating system) within Customer’s Virtual Machines. Customer may use that software only within the Microsoft Azure Services and only in conjunction with Customer’s permitted use of any applicable Microsoft Azure role, and subject to the Universal and General Terms for the software detailed in the Product Use Rights document found at <http://go.microsoft.com/?linkid=9839206> or its successor site.

[Table of Contents](#)[Introduction](#)[General Terms](#)[Privacy and Security Terms](#)[Online Service – Specific Terms](#)[Attachments](#)

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.

Import/Export Services

Customer's use of the Import/Export Service is conditioned upon its compliance with all instructions provided by Microsoft with respect to the preparation, treatment and shipment of the physical media containing its data (storage media), which will be provided via email or at www.go.microsoft.com/fwlink/?linkid=301900&CLCID=OX409. Customer is solely responsible for ensuring the storage media and data are provided in compliance with all laws and regulations. All incoming storage media will be shipped DAP Microsoft DCS Data Center (INCOTERMS 2010). Exported storage media will be shipped DAP Customer Dock (INCOTERMS 2010). Customer is responsible for ensuring that the data exported on storage media is permitted to be shipped to the location Customer provides.

Customer agrees that Microsoft has no duty with respect to the storage media and the data contained therein and no liability for lost, damaged or destroyed storage media. Customer is solely responsible for taking any precautions to protect the storage media and data contained therein, including without limitation: encrypting data, tamper-proof packaging, shipping insurance, data backup, and data redundancy.

Store

Microsoft Azure enables Customer to access or purchase Non-Microsoft Products through features such as Microsoft Azure Store and the Virtual Machine Gallery, subject to separate terms available at <http://azure.microsoft.com/en-us/support/legal/microsoft-azure-store-terms/>.

[Table of Contents](#) / [General Terms](#)

Enterprise Mobility Services

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 Rights Management, 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 Forefront Identity Manager software that is included with a Microsoft Azure Active Directory Premium User SL.

[Table of Contents](#) / [General Terms](#)

Azure Rights Management Service

[Table of Contents](#) / [General Terms](#)

Azure RemoteApp

[Table of Contents](#) / [General Terms](#)

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Privacy and Security Terms](#)



[Online Service – specific Terms](#)



[Attachments](#)

Microsoft Intune

Microsoft Intune (per user)

Manager and System Center Endpoint Protection (per user)
("Microsoft Intune Add-On")

Microsoft Intune Add-on for System Center Configuration

Manage Devices

Each user to whom Customer assigns a User SL may access and use the Online Service and related software (including System Center software) to manage up to five devices.

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 Use Rights. The Product Use Rights 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 Dynamics Online Services

Notices

The Bing Maps and Customer Support Notices in [Attachment 1](#) apply.

Subscription License Suites

In addition to User SLs, refer to [Attachment 2](#) for other offerings that fulfill SL requirements

Microsoft Dynamics CRM Online

Microsoft Dynamics CRM Online Essentials
Microsoft Dynamics CRM Online Basic

Microsoft Dynamics CRM Online Professional
Microsoft Dynamics CRM Online Enterprise

External Users

External Users of all editions of Microsoft Dynamics CRM Online do not need an SL to access the Online Service unless using Microsoft Dynamics CRM clients. This exemption does not apply to access of the Microsoft Dynamics Marketing, Microsoft Social Listening, or Parature, from Microsoft.

[Table of Contents](#) / [General Terms](#)

Microsoft Dynamics Marketing

Microsoft Dynamics Marketing Enterprise
Microsoft Dynamics Marketing Sales Collaboration

Service Level Agreement

There is no SLA for Microsoft Dynamics Marketing.

Web User Profile

Users configured and accessing this Online Service as Web Portal Users do not need User SLs.

[Table of Contents](#) / [General Terms](#)

[Table of Contents](#)

→

[Introduction](#)

→

[General Terms](#)

→

[Privacy and Security Terms](#)

→

[Online Service – specific Terms](#)

→

[Attachments](#)

Microsoft Social Listening

Microsoft Social Listening Professional

Service Level Agreement

There is no SLA for Microsoft Social Listening.

Social Content Obtained through Microsoft Social Listening

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 Listening. Social Content is not Customer Data. You may use Social Content for your 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](#)

Parature, from Microsoft

Parature Enterprise

Service Level Agreement

There is no SLA for Parature, from Microsoft.

Customer may use Parature in accordance with the privacy and/or security terms located at <http://www.parature.com/privacylegal/>.

[Table of Contents / General Terms](#)

Office 365 Services

Notices

The Bing Maps Notices in [Attachment 1](#) apply.

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.

Subscription License Suites

In addition to User SLs, refer to [Attachment 2](#) for other SLs that fulfill requirements for Exchange Online Plans 1 and 2, Lync Online Plans 1 and 2 and SharePoint Online Plans 1 and 2.

Exchange Online

Data Loss Prevention

Exchange Online Archiving for Exchange Online

Exchange Online Archiving for Exchange Server

Exchange Online Kiosk

Exchange Online Plan 1

Exchange Online Plan 2

Core Features for Office 365 Services – Exchange Online

Exchange Online or its successor service will have the following [Core Features](#) capabilities:

Emails

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Privacy and Security Terms](#)



[Online Service – specific Terms](#)



[Attachments](#)

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.

[Table of Contents / General Terms](#)

Lync Online

Lync Online Plan 1

Lync Online Plan 2

Notices

The Recording and the H.264/MPEG-4 AVC and/or VC-1 Notices in [Attachment 1](#) apply.

Core Features for Office 365 Services

Lync Online or its successor service 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 Lync Online

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

[Table of Contents / General Terms](#)

Office 365 Applications

Office 365 Business

Office 365 ProPlus

Project Pro for Office 365

Visio Pro for Office 365

Service Level Agreement

There is no SLA for Project Pro for Office 365 and Visio Pro for Office 365.

Installation and Use Rights

Each user to whom Customer assigns a 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 the software, with shared computer activation, on a network server or Microsoft Azure Platform Services and use the software to create, edit, or save documents. 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 license 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.

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 create, edit, or save documents on up to five of user's smartphones and five of user's 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.

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Privacy and Security Terms](#)



[Online Service – specific Terms](#)



[Attachments](#)

Office Web Apps Server 2013

Each Office 365 ProPlus user may use the Office Web Apps Server 2013 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](#)

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 Lite
Project Online

[Table of Contents / General Terms](#)

SharePoint Online

Duet Enterprise Online for Microsoft SharePoint and SAP
SharePoint Online Kiosk

SharePoint Online Plan 1
SharePoint Online Plan 2

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 Kiosk, 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](#)

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Privacy and Security Terms](#)



[Online Service – specific Terms](#)



[Attachments](#)

Other Online Services

Bing Maps Enterprise Platform and Bing Maps Mobile Asset Management Platform

Service SLs

A Service SL is required to provide access to the services. Each Service SL must be purchased with at least one of the following qualifying Add-On SLs:

- a Website usage Add-On SL, which is required for unauthenticated users to access Bing Maps Enterprise Platform and Bing Maps Mobile Asset Management Platform through Customer's programs based on the number of billable transactions per month,
- a public website usage SL, which is available for a specified number of billable transactions for use on a website that is available publicly without restriction,
- an Internal Website Usage Add-on, 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 Unlimited Add-on,
- Bing Maps Known User SL, or
- Bing Maps Light Known User SL.

Qualifying Bing Maps Mobile Asset Management Platform Service SL Add-on SLs

For the Bing Maps 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 Bing Maps 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 Bing Maps 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 <http://go.microsoft.com/fwlink/p/?LinkID=66121> and <http://go.microsoft.com/fwlink/p/?LinkID=223436>.

Bing Maps Privacy

The Bing Privacy Statement and privacy terms in the Microsoft Bing Maps Platform API Terms of Use located at: <http://go.microsoft.com/fwlink/?LinkID=248686> apply to Customer's use of the Bing Maps Services.

[Table of Contents / General Terms](#)

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.

[Table of Contents / General Terms](#)

Microsoft Learning IT Academy

Service SL

A Service SL is required for each Location that accesses or uses any Microsoft Learning IT 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.

IT Academy Program Guidelines

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

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Privacy and Security Terms](#)



[Online Service – specific Terms](#)



[Attachments](#)

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](#)

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](#)

Power BI for Office 365

Notices

The Bing Maps Notices in [Attachment 1](#) apply.

[Table of Contents / General Terms](#)

System Center Endpoint Protection

Device SLs

An SL is required for each device that accesses System Center Endpoint Protection or related software, excluding Servers, which require Server Management Licenses.

Server Management SLs

In addition to User SL requirements, Server Management Licenses are required for each Server in the number specified in the System Center 2012 R2 Datacenter and Standard license terms in the Management Servers section of the Product Use Rights. The Product Use Rights is located at <http://go.microsoft.com/?linkid=9839206>. For purposes of this statement, OSEs running server operating systems that access System Center Endpoint Protection or related software are managed OSEs. For this paragraph, a "Servers" is a device on which Customer runs server operating system software.

Substitution of Scan Engines

Microsoft may substitute comparable software and files for the Online Service's:

- anti-virus and anti-spam software; and
- signature files and content filtering data files.

[Table of Contents / General Terms](#)

Translator API

Customer may use Translator API in accordance with the Translator API Terms of Use, including successor Terms, located at <http://aka.ms/translatorou> and the Translator Privacy Statement located at <http://aka.ms/translatorprivacy>.

[Table of Contents / General Terms](#)

Yammer Enterprise

External Users

External Users invited to Yammer via external network functionality do not need User SLs.

Microsoft's use of Customer Data

Despite anything to the contrary in Customer's volume licensing agreement or the OST, Microsoft's use of Customer Data in the Yammer Enterprise online service, both before and after Customer's Online Service subscription terminates, will be governed by the Yammer Privacy Statement at www.yammer.com/about/privacy.

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Privacy and Security Terms](#)



[Online Service – specific Terms](#)



[Attachments](#)

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.

Customer Support

If Customer's volume licensing agreement incorporates a Master Business Agreement dated before September 1, 2007 (and Customer has not signed any other master-level Microsoft Professional Services agreement) or if Customer licenses under the Microsoft Online Subscription Agreement or other Microsoft agreement that cover Online Services only, Customer Support is provided subject to these additional terms.

Definitions

Terms used in this Customer Support Notice but not defined will have the definition provided in Customer's volume licensing agreement.

"Customer Support" means all support or advice provided to Customer under Customer's volume licensing agreement.

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

Fixes

If Microsoft provides Fixes to Customer in the course of performing Customer Support, those Fixes are licensed according to the license terms applicable to the Product to which those Fixes relate unless the Fixes include separate terms, in which case those terms will govern. If Fixes are provided for Microsoft Azure Services, Microsoft Dynamics CRM Online, Microsoft Dynamics Marketing or Microsoft Social Listening, any other use terms Microsoft provides with the Fixes will apply, and if no use terms are provided, Customer shall have a non-exclusive, temporary, fully paid-up license to use and reproduce the Fixes solely for Customer's internal use. Customer may not modify, change the file name of, or combine any Fixes with any non-Microsoft computer code.

Pre-Existing Work

All rights in any computer code or non-code based written materials developed or otherwise obtained by or for the parties or their Affiliates independent of Customer's volume licensing agreement (Pre-Existing Work) shall remain the sole property of the party providing the Pre-Existing Work. During the performance of Customer Support, each party grants to the other party (and Microsoft's contractors as necessary) a temporary, non-exclusive license to use, reproduce and modify any of its Pre-Existing Work provided to the other party, solely as needed to perform its obligations in connection with the Customer Support. Except as may be otherwise expressly agreed by the parties in writing, upon payment in full Microsoft grants Customer a non-exclusive, perpetual, fully paid-up license to use, reproduce and modify (if applicable) any Microsoft Pre-Existing Work provided as part of a Customer Support deliverable, solely in the form delivered to Customer, and solely for Customer's internal business purposes. The license to Microsoft's Pre-Existing Work is conditioned upon Customer's compliance with the terms of Customer's volume licensing agreement. If Customer is located in the Czech Republic, Customer represents that the author has granted relevant approvals to modify Customer's pre-existing work. Any violation of conditions of Customer's volume licensing agreement, or any other statements regarding customer support under that agreement, by Customer will be a condition subsequent for obtaining the perpetual license to Microsoft's Pre-existing Work that Microsoft leaves to Customer at the end of Microsoft's performance of Customer Support.

Materials

Microsoft shall own all rights in any materials developed by Microsoft (other than software code) and provided to Customer in connection with Customer Support ("Materials"), except to the extent such Materials constitute Customer's Pre-Existing Work. Microsoft grants Customer a non-exclusive, perpetual, fully paid-up license to use, reproduce and modify the Materials solely for Customer's internal business operations and without any obligation of accounting or payment of royalties.

Sample Code

Microsoft grants Customer a nonexclusive, perpetual, royalty-free right to use and modify any software code provided by Microsoft for the purposes of illustration ("Sample Code") and to reproduce and distribute the object code form of the Sample Code, provided that Customer agrees: (i) to not use Microsoft's name, logo, or trademarks to market Customer's software product in which the Sample Code is embedded; (ii) to include a valid copyright notice on Customer's software product in which the Sample Code is embedded; and (iii) to indemnify, hold harmless, and defend Microsoft and its suppliers from and against any claims or lawsuits, including attorneys' fees, that arise or result from the use or distribution of the Sample Code.

Affiliates' Rights

Customer may sublicense the rights contained in this section to Affiliates, but Customer's Affiliates may not sublicense these rights and their use must be consistent with the license terms contained in Customer's volume licensing agreement.

Warranty for Customer Support

Microsoft warrants that all Customer Support will be performed with professional care and skill.

Notice about H.264/AVC Visual Standard, VC-1 Video Standard, MPEG-4 Part 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](#)[Introduction](#)[General Terms](#)[Privacy and Security Terms](#)[Online Service – Specific Terms](#)[Attachments](#)

Attachment 2 – Subscription License Suites

Online Services may be available for purchase as Suites of Online Services. If, in the table 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.

Online Service	Office 365 Enterprise ¹				Office 365 Government				Office 365 Education				Office 365 Business Essentials	Office 365 Business Premium	Office 365 Midsize Business	Enterprise Mobility Suite	Enterprise Cloud Suite ²	Microsoft Dynamics CRM Online	
	K1	E1	E3	E4	K1	E1	E3	E4	E1	E3	E4	Pro.						Ent.	
Exchange Online																			
Exchange Online Kiosk																			
Exchange Online Plan 1																			
Exchange Online Plan 2																			
SharePoint Online																			
SharePoint Online Kiosk																			
SharePoint Online Plan 1																			
SharePoint Online Plan 2																			
Lync Online																			
Lync Online Plan 1																			
Lync Online Plan 2																			
Yammer Enterprise																			
Office Online																			
Office 365 Business																			
Office 365 ProPlus																			
Microsoft Intune																			
Azure Rights Management																			
Azure Active Directory Premium																			
Microsoft Dynamics Marketing Sales Collaboration																			
Microsoft Dynamics Marketing Enterprise																			
Microsoft Social Listening Professional																			
Parature Enterprise																			

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 Enterprise Cloud Suite fulfills the SL requirement for Windows SA per User as described in the Product List. The Product List is located at <http://go.microsoft.com/?linkid=9839207>.

Attachment 3 – The Standard Contractual Clauses (Processors)

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.

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 or 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

[Table of Contents](#)



[Introduction](#)



[General Terms](#)



[Privacy and Security Terms](#)



[Online Service – Specific Terms](#)



[Attachments](#)

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 "Security and Data Processing: Additional Technical and Organizational Measures."

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

Data subjects: Data subjects include the data exporter's customer'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 DPT. 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 Data without authorization. Personnel are obligated to maintain the confidentiality of any 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 DPT, 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 DPT 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.

[Table of Contents](#)[Introduction](#)[General Terms](#)[Privacy and Security Terms](#)[Online Service – Specific Terms](#)[Attachments](#)

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

Signature  ..DocuSigned By: Rajesh Jha..

The signature box is a blue-bordered rectangle containing the handwritten name "Rajesh Jha" in black ink. Above the name is the alphanumeric string "851B7BFC2840456". Below the name is the text "DocuSigned By: Rajesh Jha..". A dotted line extends from the right side of the signature box.

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