Microsoft Online Subscription Agreement Amendment adding Office 365 Data Processing Agreement

Amendment ID MOS02

To be valid, Customer must have accepted this Amendment as set forth in the Office 365 online portal.

This amendment ("Amendment") is between the customer entity ("Customer") and the Microsoft entity ("Microsoft") who are party to the Microsoft Online Subscription Agreement ("Agreement") under which Customer has purchased Office 365 Services. The parties agree that the Amendment supplements the Agreement and applies to only the Office 365 Services, defined below, Customer buys under the Agreement.

Defined Terms

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

"Customer Data" means all data, including all text, sound, or image files that are provided to Microsoft by, or on behalf of, Customer through Customer's use of the Office 365 Services.

"End User" means an individual that accesses the Office 365 Services.

"Office 365 Services" means Office 365 Plans E1, E2, E3, E4, P1, K1 and K2; Exchange Online Plan 1, Plan 2 and Kiosk; SharePoint Online Plans 1 and 2; Office Web Apps Plans 1 and 2; and Lync Online Plans 1 and 2.

1. Privacy.

a. Privacy practices. Microsoft complies with all data protection and privacy laws generally applicable to Microsoft's provision of the Office 365 Services. However, Microsoft is not responsible for compliance with any data protection or privacy law applicable to Customer or its industry and not generally applicable to information technology service providers.

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

(i) Customer Data will be used only to provide Customer the Office 365 Services. This may include troubleshooting aimed at preventing, detecting and repairing problems affecting the operation of the Office 365 Services and the improvement of features that involve the detection of, and protection against, emerging and evolving threats to the user (such as malware or spam).

(ii) Microsoft will not disclose Customer Data to law enforcement unless required by law. Should law enforcement contact Microsoft with a demand for Customer Data, it will attempt to redirect the law enforcement agency to request it directly from Customer. As part of this effort, Microsoft may provide Customer's basic contact information to the agency. If compelled to disclose Customer Data to law enforcement, Microsoft will use commercially reasonable efforts to notify Customer in advance of a disclosure unless legally prohibited.

c. **Customer Data deletion or return.** Upon expiration or termination of Customer's use of the Office 365 Services, Customer may extract Customer Data and Microsoft will delete Customer Data, each in accordance with the Product Use Rights.

d. **End User requests**. Microsoft will not independently respond to requests from Customer's End Users without Customer's prior written consent, except where required by applicable law.

e. **Transfer of Customer Data; appointment.** 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 Office 365 Services. Microsoft (1) 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, and (2) will, during the Term of the Subscription for the Office 365 Services, remain certified under the EU and Swiss Safe Harbor programs so long as they are maintained by the United States government.

f. **Microsoft personnel.** Microsoft personnel will not process Customer Data without authorization. Microsoft personnel are obligated to maintain the confidentiality of any Customer Data and this obligation continues even after their engagement ends.

g. **Subcontractor; transfer.** Microsoft may hire other companies to provide limited services on its behalf, such as providing customer support. Any such subcontractors will be permitted to obtain Customer Data only to deliver the services Microsoft has retained them to provide, and they are prohibited from using Customer Data for any other purpose. Microsoft remains responsible for its subcontractors' compliance with the obligations of this Amendment. Any subcontractors to whom Microsoft transfers Customer Data will have entered into written agreements with Microsoft requiring that the subcontractor provide at least the same level of privacy protection with respect to personal data received from Microsoft as is required by the relevant Safe Harbor principles. Customer consents to Microsoft's transfer of Customer Data to subcontractors as described in this Amendment. Except as set forth above, 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 Office 365 Services.

2. Customer responsibilities.

Customer must comply with applicable legal requirements for privacy, data protection, and confidentiality of communications related to its use of Office 365 Services.

3. Additional European terms.

If Customer has End Users in the European Economic Area or Switzerland, the additional terms in this Section 3 will apply. Terms used in this Section that are not specifically defined will have the meaning in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("EU Data Protection Directive").

a. **Intent of the parties.** For the Office 365 Services, Customer is the data controller and Microsoft is a data processor acting on Customer's behalf. As data processor, Microsoft will only act upon Customer's instructions. This Amendment and the Agreement (including the terms and conditions incorporated by reference therein) are Customer's complete and final instructions to Microsoft for the processing of Customer Data. Any additional or alternate instructions must be agreed to according to the process for amending Customer's Agreement.

b. **Duration and object of data processing.** The duration of data processing shall be for the Term of the Subscription for the Office 365 Services. The objective of the data processing is the performance of the Office 365 Services.

c. 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 this Amendment and the Agreement.

d. Customer Data access. For the Term of the Subscription for the Office 365 Services 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.

e. Privacy officer. Microsoft's data privacy representative for the European Economic Area and Switzerland can be reached at the following address:

Microsoft Ireland Operations Ltd.
Attn: Privacy Officer
Carmenhall Road
Sandyford, Dublin 18, Ireland

4. Security.

a. General practices. Microsoft has implemented and will maintain appropriate technical and organizational measures, internal controls, and information security routines intended to protect Customer Data against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction as follows:

(i) Domain: organization of information security

1) Security ownership. Microsoft has appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures.

2) Security roles and responsibilities. Microsoft personnel with access to Customer Data are subject to confidentiality obligations.

3) Risk management program. Microsoft performed a risk assessment before processing the Customer Data or launching the Office 365 Service.

4) Microsoft retains its security documents pursuant to its retention requirements after they are no longer in effect.

(ii) Domain: asset management

1) 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.

2) Asset handling.

A. Microsoft classifies Customer Data to help identify it and to allow for access to it to be appropriately restricted (e.g., through encryption).

B. Microsoft imposes restrictions on printing Customer Data and has procedures for disposing of printed materials that contain Customer Data.

C. 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. This includes removing media (e.g., USB sticks and CD ROMs) and documents containing Customer Data from Microsoft's facilities.

(iii) Domain: human resources security.

1) Security training.

A. 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.

B. Microsoft will only use anonymous data in training.

(iv) Domain: physical and environmental security.

1) **Physical access to facilities.** Microsoft limits access to facilities where information systems that process Customer Data are located to identified authorized individuals.

2) **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.

3) **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.

4) **Component disposal.** Microsoft uses industry standard processes to delete Customer Data when it is no longer needed.

(v) Domain: communications and operations management.

1) **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.

2) **Data recovery procedures.**

A. 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.

B. 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.

C. Microsoft has specific procedures in place governing access to copies of Customer Data.

D. Microsoft reviews data recovery procedures at least every six months.

E. Microsoft logs data restoration efforts, including the person responsible, the description of the restored data and which data (if any) had to be input manually in the data recovery process.

3) **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.

4) **Data beyond boundaries.**

A. Microsoft encrypts Customer Data that is transmitted over public networks.

B. Microsoft restricts access to Customer Data in media leaving its facilities (e.g., through encryption).

(vi) Domain: a**ccess control.**

1) **Access policy.** Microsoft maintains a record of security privileges of individuals having access to Customer Data.

2) **Access authorization.**

A. Microsoft maintains and updates a record of personnel authorized to access Microsoft systems that contain Customer Data.

B. Microsoft deactivates authentication credentials that have not been used for a period of time not to exceed six months.

C. Microsoft identifies those personnel who may grant, alter or cancel authorized access to data and resources.

3) **Least privilege.**

A. Technical support personnel are only permitted to have access to Customer Data when needed.

B. Microsoft restricts access to Customer Data to only those individuals who require such access to perform their job function.

4) **Integrity and confidentiality.**

A. Microsoft instructs Microsoft personnel to disable administrative sessions when leaving premises Microsoft controls or when computers are otherwise left unattended.

5) **Authentication.**

A. Microsoft uses industry standard practices to identify and authenticate users who attempt to access information systems.

B. Where authentication mechanisms are based on passwords, Microsoft requires that the passwords are renewed regularly.

C. Where authentication mechanisms are based on passwords, Microsoft requires the password to be at least eight characters long.

D. Microsoft ensures that de-activated or expired identifiers are not granted to other individuals.

E. Microsoft monitors repeated attempts to gain access to the information system using an invalid password.

F. Microsoft maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed.

G. 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.

6) **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.

(vii) Domain: information security incident management

1) **Incident response process.** Microsoft maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data.

2) **Service Monitoring.** Microsoft security personnel verify logs at least every six months to propose remediation efforts if necessary.

(viii) Domain: Business Continuity Management

1) Microsoft maintains emergency and contingency plans for the facilities in which Microsoft information systems that process Customer Data are located.

2) Microsoft's redundant storage and its procedures for recovering data are designed to attempt to reconstruct Customer Data in its original state from before the time it was lost or destroyed.

(ix) The security measures described in this Section 4 are Microsoft's only responsibility with respect to the security of Customer Data. For Customer Data, these measures replace any confidentiality obligations contained in the Agreement or any other non-disclosure agreement between Microsoft and Customer.

b. Certifications and audits.

(i) Microsoft has established and agrees to maintain a data security policy that complies with the ISO 27001 standards for the establishment, implementation, control, and improvement of the Information Security Management System and the ISO/IEC

27002 code of best practices for information security management ("Microsoft Online Information Security Policy"). On a confidential need-to-know basis, and subject to Customer's agreement to non-disclosure obligations Microsoft specifies, Microsoft will make the Microsoft 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 Microsoft Online Information Security Policy, making an independent determination as to whether the Microsoft 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.

(ii) Microsoft will audit the security of the computers and computing environment that it uses in processing Customer Data (including personal data) on the Office 365 Services and the physical data centers from which Microsoft provides the Office 365 Services. This audit: (1) will be performed at least annually; (2) will be performed according to ISO 27001 standards; (3) will be performed by 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).

(iii) If Customer requests in writing, Microsoft will provide Customer with a confidential summary of the Microsoft Audit Report ("Summary Report") so that Customer can reasonably verify Microsoft's compliance with the security obligations under this Amendment. The Summary Report is Microsoft confidential information.

(iv) Microsoft will make good faith, commercially reasonable efforts to remediate (1) any errors identified in a Microsoft Audit Report that could reasonably be expected to have an adverse impact on Customer use of the Office 365 Services and (2) material control deficiencies identified in the Microsoft Audit Report.

5. Miscellaneous.

a. Confidentiality. Customer will treat the terms and conditions of this Amendment, the contents of the Microsoft Online Information Security Policy, the Microsoft Audit Report and the Summary Report as confidential and shall not disclose them to any third party except for Customer's auditors or consultants that need access to this information for the purpose of this business relationship as articulated in this Amendment and the Agreement.

b. Term and termination. This Amendment shall automatically terminate upon any termination or expiration of the Agreement.

c. Order of precedence. If there is a conflict between any provision in this Amendment and any provision in the Agreement, this Amendment shall control.

d. Entire agreement. Except for changes made by this Amendment, the Agreement remains unchanged and in full force and effect.