Online Service DPA

Table of Contents

Volume Licensing

Microsoft Online Services Data Protection Addendum January 2020

Microsoft

Introduction

The parties agree that this Microsoft Online Services Data Protection Addendum ("DPA") sets forth their obligations with respect to the processing and security of Customer Data and Personal Data in

connection with the Online Services. The parties also agree that, unless a separate Professional Services agreement exists, this DPA governs the processing and security of Professional Services Data. Separate terms, including different privacy and security terms, govern Customer's use of Non-Microsoft Products.

In the event of any conflict or inconsistency between this DPA and any other terms in Customer's volume licensing agreement (including the

Product Terms or the Online Services Terms), this DPA shall prevail. The provisions of this DPA supersede any conflicting provisions of the Microsoft Privacy Statement that otherwise may apply to processing of Customer Data, Personal Data, or Professional Services Data as defined herein. For clarity, consistent with Clause 10 of the Standard Contractual Clauses in **Attachment 2**, the Standard Contractual Clauses prevail over any other term of the DPA.

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

Applicable DPA and Updates

When Customer renews or purchases a new subscription to an Online Service, the then-current DPA will apply and will not change during

Customer's subscription for that Online Service. When Microsoft introduces features, supplements or related software that are new (i.e., that were not previously included with the subscription), Microsoft may provide terms or make updates to the DPA that apply to Customer's use of those new features, supplements or related software.

Electronic Notices

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

Prior Versions

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

Clarifications and Summary of Changes

Definitions

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

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

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

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

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

Customer Data does not include Professional Services Data.

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

"GDPR Terms" means the terms in **Attachment 3**, under which Microsoft makes binding commitments regarding its processing of Personal Data as required by Article 28 of the GDPR.

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

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

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

Professional Services Data includes Support Data.

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

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

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

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

Table of Contents / General Terms

General Terms

Compliance with Laws

Microsoft will comply with all laws and regulations applicable to its provision of the Online Services, including security breach notification law and

Data Protection Requirements. However, Microsoft is not responsible for compliance with any laws or regulations applicable to Customer or

Customer's industry that are not generally applicable to information technology service providers. Microsoft does not determine whether

Customer Data includes information subject to any specific law or regulation. All Security Incidents are subject to the Security Incident Notification terms below.

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

Data Protection Terms

This section of the DPA includes the following subsections:

Scope

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

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

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

Nature of Data Processing; Ownership

Microsoft will use and otherwise process Customer Data and Personal Data only (a) to provide Customer the Online Services in accordance with Customer's documented instructions, and (b) for Microsoft's legitimate business operations, each as detailed and limited below. As between the parties, Customer retains all right, title and interest in and to Customer Data. Microsoft acquires no rights in Customer Data, other than the rights

Customer grants to Microsoft in this section. This paragraph does not affect Microsoft's rights in software or services Microsoft licenses to Customer.

Processing to Provide Customer the Online Services

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

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

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

Processing for Microsoft's Legitimate Business Operations

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

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

Disclosure of Processed Data

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

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

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

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

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

Processing of Personal Data; GDPR

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

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

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

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

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

Processing Details

The parties acknowledge and agree that:

- **Subject Matter.** The subject-matter of the processing is limited to Personal Data within the scope of the section of this DPA entitled "Nature of Data Processing; Ownership" above and the GDPR.

- **Duration of the Processing.** The duration of the processing shall be in accordance with Customer instructions and the terms of the DPA.

- **Nature and Purpose of the Processing.** The nature and purpose of the processing shall be to provide the Online Service pursuant to Customer's volume licensing agreement (as further described in the section of this DPA entitled "Nature of Data Processing; Ownership" above).

- **Categories of Data.** The types of Personal Data processed by the Online Service include: (i) Personal Data that Customer elects to include in

Customer Data; and (ii) those expressly identified in Article 4 of the GDPR that may be contained in Diagnostic Data or Service Generated Data. The types of Personal Data that Customer elects to include in Customer Data may be any categories of Personal Data identified in records maintained by Customer acting as controller pursuant to Article 30 of the GDPR, including the categories of Personal Data set forth in **Appendix 1 to Attachment 2** – The Standard Contractual Clauses (Processors) of the DPA.

- **Data Subjects.** The categories of data subjects are Customer's representatives and end users, such as employees, contractors, collaborators, and customers, and may include any other categories of data subjects as identified in records maintained by Customer acting as controller pursuant to Article 30 of the GDPR, including the categories of data subjects set forth in **Appendix 1 to Attachment 2** – The Standard Contractual Clauses (Processors) of the DPA.

Data Subject Rights; Assistance with Requests

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

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

Data Security

Security Practices and Policies

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

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

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

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

Auditing Compliance

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

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

Each audit will result in the generation of an audit report ("Microsoft Audit Report"), which Microsoft will make available at https://servicetrust.microsoft.com/ or another location identified by

Microsoft. The Microsoft Audit Report will be Microsoft's Confidential Information and will clearly disclose any material findings by the auditor. Microsoft will promptly remediate issues raised in any Microsoft Audit Report to the satisfaction of the auditor. If Customer requests, Microsoft will provide Customer with each Microsoft Audit Report. The Microsoft Audit Report will be subject to non-disclosure and distribution limitations of Microsoft and the auditor.

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

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

Security Incident Notification

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

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

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

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

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

Data Transfers and Location

Data Transfers

Except as described elsewhere in the DPA, Customer Data and Personal Data that Microsoft processes on Customer's behalf may be transferred to, and stored and processed in, the United States or any other country in which Microsoft or its Subprocessors operate. Customer appoints Microsoft to perform any such transfer of Customer Data and Personal Data to any such country and to store and process Customer Data and Personal Data to provide the Online Services.

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

Microsoft will abide by the requirements of European Economic Area and Swiss data protection law regarding the collection, use, transfer, retention, and other processing of Personal Data from the European Economic Area and Switzerland. All transfers of Personal Data to a third country or an international organization will be subject to appropriate safeguards as described in Article 46 of the GDPR and such transfers and safeguards will be documented according to Article 30(2) of the GDPR.

In addition, Microsoft is certified to the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks and the commitments they entail. Microsoft agrees to notify Customer if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Privacy Shield principles.

Location of Customer Data at Rest

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

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

Data Retention and Deletion

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

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

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

Processor Confidentiality Commitment

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

Notice and Controls on use of Subprocessors

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

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

From time to time, Microsoft may engage new Subprocessors. Microsoft will give Customer notice (by updating the website and providing

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

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

Educational Institutions

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

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

CJIS Customer Agreement

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

HIPAA Business Associate

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

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

California Consumer Privacy Act (CCPA)

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

How to Contact Microsoft

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

Microsoft Enterprise Service Privacy

Microsoft Corporation

One Microsoft Way

Redmond, Washington 98052 USA

Microsoft Ireland Operations Limited is Microsoft's data protection representative for the European Economic Area and Switzerland. The privacy representative of Microsoft Ireland Operations Limited can be reached at the following address:

Microsoft Ireland Operations, Ltd.

Attn: Data Protection

One Microsoft Place

South County Business Park

Leopardstown

Dublin 18, D18 P521, Ireland

Table of Contents / General Terms

Appendix A – Security Measures

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

Domain	Practices
Organization of Information Security	**Security Ownership.** Microsoft has appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures. **Security Roles and Responsibilities.** Microsoft personnel with access to Customer Data are subject to confidentiality obligations. **Risk Management Program.** Microsoft performed a risk assessment before processing the Customer Data or launching the Online Services service. Microsoft retains its security documents pursuant to its retention requirements after they are no longer in effect.
Asset Management	**Asset Inventory.** Microsoft maintains an inventory of all media on which Customer Data is stored. Access to the inventories of such media is restricted to Microsoft personnel authorized in writing to have such access. **Asset Handling** - Microsoft classifies Customer Data to help identify it and to allow for access to it to be appropriately restricted. - Microsoft imposes restrictions on printing Customer Data and has procedures for disposing of printed materials that contain Customer Data. - Microsoft personnel must obtain Microsoft authorization prior to storing Customer Data on portable devices, remotely accessing Customer Data, or processing Customer Data outside Microsoft's facilities.
Human Resources Security	**Security Training.** Microsoft informs its personnel about relevant security procedures and their respective roles. Microsoft also informs its personnel of possible consequences of breaching the security rules and procedures. Microsoft will only use anonymous data in training.
Physical and Environmental Security	**Physical Access to Facilities.** Microsoft limits access to facilities where information systems that process Customer Data are located to identified authorized individuals. **Physical Access to Components.** Microsoft maintains records of the incoming and outgoing media containing Customer Data, including the kind of media, the authorized sender/recipients, date and time, the number of media and the types of Customer Data they contain. **Protection from Disruptions.** Microsoft uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference. **Component Disposal.** Microsoft uses industry standard processes to delete Customer Data when it is no longer needed.
Communications and Operations Management	**Operational Policy.** Microsoft maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Customer Data. **Data Recovery Procedures** - On an ongoing basis, but in no case less frequently than once a week (unless no Customer Data has been updated during that period), Microsoft maintains multiple copies of Customer Data from which Customer Data can be recovered. - Microsoft stores copies of Customer Data and data recovery procedures in a different place from where the primary computer equipment processing the Customer Data is located. - Microsoft has specific procedures in place governing access to copies of Customer Data. - Microsoft reviews data recovery procedures at least every six months, except for data recovery procedures for Azure Government Services, which are reviewed every twelve months. - Microsoft logs data restoration efforts, including the person responsible, the description of the restored data and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process. **Malicious Software.** Microsoft has anti-malware controls to help avoid malicious software gaining unauthorized access to Customer Data, including malicious software originating from public networks. **Data Beyond Boundaries**

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

Table of Contents / General Terms

Attachment 1 – Notices

Professional Services

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

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

Processing of Professional Services Data; Ownership

Microsoft will use and otherwise process Professional Services Data only (a) to provide Customer the Professional Services in accordance with the Customer's documented instructions, and (b) for Microsoft's legitimate business operations, each as detailed and limited below. As between the

parties, Customer retains all right, title and interest in and to Professional Services Data. Microsoft acquires no rights in Professional Services Data, other than the rights Customer grants to Microsoft to provide the Professional Services to Customer. This paragraph does not affect Microsoft's rights in software or services Microsoft licenses to Customer.

Processing to Provide Customer the Professional Services

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

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

When providing Professional Services, Microsoft will not use or otherwise process Professional Services Data for: (a) user profiling,

(b) advertising or similar commercial purposes, or (c) market research aimed at creating new functionalities, services, or products or any other purpose, unless such use or processing is in accordance with Customer's documented instructions. **Processing for Microsoft's Legitimate Business Operations**

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

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

Disclosure of Professional Services Data

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

Processing of Personal Data; GDPR

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

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

Customer and Microsoft agree that Customer is the controller of Personal Data included in Professional Services Data and Microsoft is the processor, except (a) when Customer acts as a

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

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

The parties acknowledge and agree that:

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

Data Subject Rights; Assistance with Requests

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

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

Data Security

Security Practices and Policies

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

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

Security Incident Notification

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

Data Transfers

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

Data Deletion or Return

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

Processor Confidentiality Commitment

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

Notice and Controls on use of Subprocessors

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

Microsoft is responsible for its Subprocessors of Professional Services Data compliance with Microsoft's obligations in **Attachment 1** of the DPA. Microsoft will ensure via a written contract that the Subprocessor may access and use Professional Services Data only to deliver the services

Microsoft has retained them to provide and is prohibited from using Professional Services Data for any other purpose. Microsoft will ensure that Subprocessors are bound by written agreements that require them to provide at least the level of data protection required of Microsoft by these Professional Services Terms. Microsoft agrees to oversee the Subrpocessors to ensure that these contractual obligations are met.

With respect to Professional Services Data other than Support Data, a list of Microsoft's Subprocessors is available upon request. If such list is requested, at least 30 days before authorizing any new Subprocessor to access Personal Data, Microsoft will update the list and provide Customer with a mechanism to obtain notice of that update.

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

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

Additional Terms for Support Data

Security of Support Data

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

Educational Institutions

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

California Consumer Privacy Act (CCPA)

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

any data protection commitments Microsoft makes to Customer in the DPA, Online Services Terms, or other agreement between Microsoft and Customer.

Table of Contents / General Terms

Attachment 2 – The Standard Contractual Clauses (Processors)

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

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

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

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

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

1. '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;
2. 'the data exporter' means the controller who transfers the personal data;
3. '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;
4. '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;

5. '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;

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

Clause 2: Details of the transfer

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

Clause 3: Third-party beneficiary clause

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

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

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

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

Clause 4: Obligations of the data exporter The data exporter agrees and warrants:

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

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

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

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

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

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

95/46/EC;

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

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

(i. that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and (j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5: Obligations of the data importer The data importer agrees and warrants:

1. 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;

2. 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;

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

4. that it will promptly notify the data exporter about:

    a. 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,

    b. any accidental or unauthorised access, and

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

5. 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;

6. 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;

7. 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;

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

9. that the processing services by the subprocessor will be carried out in accordance with Clause 11; and

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

Clause 6: Liability

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

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

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

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

Clause 7: Mediation and jurisdiction

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

(a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority; (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

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

Clause 8: Cooperation with supervisory authorities

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

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

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

Clause 9: Governing Law.

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

Clause 10: Variation of the contract

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

Clause 11: Subprocessing

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

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

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

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to

Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

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

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

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

Appendix 1 to the Standard Contractual Clauses

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

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

Data subjects: Data subjects include the data exporter's representatives and end-users including employees, contractors, collaborators, and customers of the data exporter. Data subjects may also include individuals attempting to communicate or transfer personal information to users of the services provided by data importer. Microsoft acknowledges that, depending on Customer's use of the Online Service, Customer may elect to include personal data from any of the following types of data subjects in the Customer Data:

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

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

- Basic personal data (for example place of birth, street name and house number (address), postal code, city of residence, country of residence, mobile phone number, first name, last name, initials, email address, gender, date of birth), including basic personal data about family members and children;
- Authentication data (for example user name, password or PIN code, security question, audit trail);
- Contact information (for example addresses, email, phone numbers, social media identifiers; emergency contact details);
- Unique identification numbers and signatures (for example Social Security number, bank account number, passport and ID card number, driver's license number and vehicle registration data, IP addresses, employee number, student number, patient number, signature, unique identifier in tracking cookies or similar technology);
- Pseudonymous identifiers;
- Financial and insurance information (for example insurance number, bank account name and number, credit card name and number, invoice number, income, type of assurance, payment behavior, creditworthiness);

• Commercial Information (for example history of purchases, special offers, subscription information, payment history);

• Biometric Information (for example DNA, fingerprints and iris scans);

• Location data (for example, Cell ID, geo-location network data, location by start call/end of the call. Location data derived from use of wifi access points);

• Photos, video and audio;

• Internet activity (for example browsing history, search history, reading, television viewing, radio listening activities);

• Device identification (for example IMEI-number, SIM card number, MAC address);

• Profiling (for example based on observed criminal or anti-social behavior or pseudonymous profiles based on visited URLs, click streams, browsing logs, IP-addresses, domains, apps installed, or profiles based on marketing preferences);

• HR and recruitment data (for example declaration of employment status, recruitment information (such as curriculum vitae, employment history, education history details), job and position data, including worked hours, assessments and salary, work permit details, availability, terms of employment, tax details, payment details, insurance details and location and organizations);

• Education data (for example education history, current education, grades and results, highest degree achieved, learning disability);

• Citizenship and residency information (for example citizenship, naturalization status, marital status, nationality, immigration status, passport data, details of residency or work permit);

• Information processed for the performance of a task carried out in the public interest or in the exercise of an official authority;

• Special categories of data (for example racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, data concerning a natural person's sex life or sexual orientation, or data relating to criminal convictions or offences); or

• Any other personal data identified in Article 4 of the GDPR.

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

1. **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.

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

3. **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.

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

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

Subcontractors: In accordance with the DPA, the data importer may hire other companies to provide limited services on data importer's behalf, such as providing customer support. Any such subcontractors will be permitted to obtain Customer Data only to deliver the services the data importer has retained them to provide, and they are prohibited from using Customer Data for any other purpose. **Appendix 2 to the Standard Contractual Clauses**

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

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

2. Data Privacy Contact. The data privacy officer of the data importer can be reached at the following address:

Microsoft Corporation

Attn: Chief Privacy Officer

1 Microsoft Way

Redmond, WA 98052 USA

3. Technical and Organization Measures. The data importer has implemented and will maintain appropriate technical and organizational measures, internal controls, and information security routines intended to protect Customer Data, as defined in the Security Practices and Policies section of the DPA, against accidental loss, destruction, or alteration; unauthorized disclosure or access; or unlawful destruction as follows: The technical and organizational measures, internal controls, and information security routines set forth in the Security Practices and Policies section of the DPA are hereby incorporated into this Appendix 2 by this reference and are binding on the data importer as if they were set forth in this Appendix 2 in their entirety.

Signature of Microsoft Corporation appears on the following page.

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

Signature 

Rajesh Jha, Corporate Vice President

Microsoft Corporation

One Microsoft Way, Redmond WA, USA 98052

Table of Contents / General Terms

Attachment 3 – European Union General Data Protection Regulation

Terms

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

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

Relevant GDPR Obligations: Articles 28, 32, and 33

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

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

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

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

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

(d. respect the conditions referred to in paragraphs 1 and 3 for engaging another processor;

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

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

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

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

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

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

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

(a. the pseudonymisation and encryption of Personal Data;

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

(c. the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and

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

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

(Article 32(2))

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

7. Microsoft shall notify Customer without undue delay after becoming aware of a Personal Data breach. (Article 33(2)). Such notification will include that information a processor must provide to a controller under Article 33(3) to the extent such information is reasonably available to Microsoft.

Table of Contents / General Terms