Příloha 1 - Google Apps Enterprise Online Agreement

This Google Apps Enterprise Agreement (the "**Agreement**") is entered into by and between the entity or person agreeing to these terms ("**Customer**") and one of the following Google entities (as applicable "**Google**"): (a) Google Ireland Limited, a company incorporated under the laws of Ireland with offices at Gordon House, Barrow Street, Dublin 4, Ireland; or (b) if Customer resides in the EU and has chosen "non-business" as the tax status/setting for its Google account, Google Commerce Limited, a company incorporated under the laws of Ireland with offices at Gordon House, Barrow Street, Dublin 4, Ireland ("**GCL**"). This Agreement is effective as of the date on which Customer clicks the "I Accept" button below (the "**Effective Date**"). If you are accepting on behalf of Customer, you represent and warrant that you: (i) have full legal authority to bind Customer to these terms and conditions; (ii) have read and understood this Agreement; and (iii) agree to this Agreement on behalf of Customer. If you do not have the legal authority to bind Customer, please do not click the "I Accept" button below. This Agreement governs Customer's access to and use of the Services.

- 1. **Services.**

1.1 **General.** Google will provide the Services in accordance with this Agreement including the SLA. Google will provide Customer with an Admin Account to use for administering the End User Accounts and other features of the Services. Customer shall: administer End User Accounts using the Admin Console and Admin Tools, and determine the Services to be provided to End Users. Customer may request End User Accounts by: (a) notifying its designated Google account manager; or (b) ordering End User Accounts via the Admin Console.

1.2 **Modifications to the Services.** Google may make commercially reasonable changes to the Services from time to time. If Google makes a material change to the Services, Google will inform Customer via such method as Google may elect provided that Customer has subscribed with Google to be informed about such changes.

1.3 **Modifications to URL Terms.** Google may make commercially reasonable changes to the URL Terms from time to time. If Google makes a material change to any of the URL Terms, Google will inform Customer by either sending an email to the Notification Email Address or alerting Customer via the Admin Console. Any such

change to the URL Terms will take effect 30 days after Customer is informed of it, unless Customer is on an Annual Plan, and the change has a material adverse impact on Customer, in which case if Customer notifies Google via the Help Centre of Customer's objection to the change within 30 days after being informed of it Customer will remain governed by the terms in effect immediately prior to the change until the end of the then-current Services Term for the affected Services. If the affected Services are then renewed in accordance with this Agreement, they will be renewed under Google's then current URL Terms.

- 2. **Data Processing.**

2.1 **Data Protection Legislation.** In this Agreement the terms "**personal data**", "**processing**", "**controller**" and "**processor**" shall have the meanings ascribed to them in the EU Directive. The parties agree and acknowledge that the Data Protection Legislation applies to the processing of Customer Data.

2.2 **Processor.** For the purposes of this Agreement and in respect of Customer Data, the parties agree that Customer shall be the controller and Google shall be a processor. Customer shall comply with its obligations as a controller and Google shall comply with its obligations as a processor under the Agreement. Where a Customer Group Company is the controller (either alone or jointly with the Customer) with respect to certain Customer Data, Customer represents and warrants to Google that it is authorized to instruct Google and otherwise act on behalf of such Customer Group Company in relation to the Customer Data in accordance with the Agreement, as amended.

2.3 **Scope of Processing.** Customer instructs Google to process Customer Data for the following purposes: (a) to comply with Instructions, (b) to provide the Services (as selected by the Customer via the Admin Console); (c) to provide product features to facilitate Customer's use of Services and tools for the Customer to create content; (d) to operate, maintain and support the infrastructure used to provide the Services; and (e) to respond to customer support requests. Google will only process Customer Data in accordance with this Agreement and will not process Customer Data for any other purpose. Google only processes Customer Data that is transmitted by Customer or End Users via the Services.

2.5 **Data Security.** Google will take and implement appropriate technical and organisational measures to protect Customer Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access ("**Security Measures**").

2.6 **Google Staff.** Google will take appropriate steps to ensure compliance with the Security Measures by its employees, contractors and Subprocessors to the extent applicable to their scope of performance.

2.8 **Security Certification.** During the Term, Google will maintain its ISO/IEC 27001:2005 Certification or a comparable certification ("**ISO Certification**") for the Services.

2.9 **Security Audit.** During the Term, Google will maintain its Statement on Standards for Attestation Engagements (SSAE) No. 16 Type II / International Standards for Assurance Engagements (ISAE) No. 3402 report (or a comparable report) on Google's systems examining logical security controls, physical security controls, and system availability ("**Audit Report**") as related to the Services. At least every 18 months, Google will instruct a third party to produce an updated Audit Report. A summary of the Audit Report is available on Google's website.

2.10 **Data Correction, Blocking and Deletion.** For the term of the Agreement Google will provide Customer or End Users with the ability to correct, block, export and delete Customer Data in a manner consistent with the functionality of the Services. Once Customer or End User deletes Customer Data (and such Customer Data cannot be recovered by the Customer or End User, such as from the "trash") Google will delete such Customer Data from its systems as soon as reasonably practicable and within a maximum period of 180 days.

2.11 **Access to Data.** Google will make available to Customer the Customer Data in accordance with the terms of the Agreement in a manner consistent with the functionality of the Services, including the applicable SLA. To the extent Customer, in its use and administration of the Services, does not have the ability to amend or delete Customer Data, (as required by applicable law) or migrate Customer Data to another system or service provider, Google will comply with any reasonable requests by Customer to assist in facilitating such actions to the extent Google is legally permitted to do so and has reasonable access to the Customer Data.

2.12 **Data Privacy Officer.** The Data Privacy Officer of Google can be contacted at: enterprise-dpo@google.com.

2.13 **Data Transfers.** As part of providing the Services, Google may transfer, store and process Customer Data in the United States or any other country in which Google or its Group Companies maintain facilities.

2.14 **Safe Harbor.** During the Term, Google Inc., will remain enrolled in the U.S Department of Commerce Safe Harbor Program ("**Safe Harbor**") or will adopt an alternative compliance solution that achieves compliance with the terms of the Directive for transfers of personal data to a third country. While Google Inc. remains enrolled in Safe Harbor: (i) the scope of Google Inc.'s Safe Harbor certification will include Customer Data; and (ii) the Google Group's processing practices in respect of Customer Data will remain consistent with those described in Google Inc.'s Safe Harbor certification and the Safe Harbor Privacy Principles.

2.15 **Subprocessors.** Google may engage Subprocessors to provide limited parts of the Services. Google will ensure that Subprocessors only access and use Customer Data in accordance with the terms of the Agreement and that they are bound by written obligations that require them to provide at least the level of data protection required by the Safe Harbor Privacy Principles. Customer consents to Google subcontracting the processing of Customer Data to Subprocessors in accordance with the terms of the Agreement. At the written request of the Customer, Google will provide additional information regarding Third Party Suppliers and their locations. Customer will send such requests to the Data Privacy Officer at: enterprise-dpo@google.com.

- 7. **Confidential Information.**

7.1 The recipient of any Confidential Information will not disclose that Confidential Information, except to Group Companies, Subprocessors, employees and/or professional advisors who need to know it and who have agreed in writing (or in the case of professional advisors are otherwise bound) to keep it confidential. The recipient will ensure that those people and entities may use such Confidential Information only to exercise rights and fulfil obligations under this Agreement, while using reasonable care to protect it. The recipient may also disclose Confidential Information when required by law after giving reasonable notice, if legally permissible, to the discloser. Any such notice will be sufficient to give the discloser the opportunity

to seek confidential treatment, a protective order or similar remedies or relief prior to disclosure.

7.2 Confidential Information does not include information that: (a) the recipient of the Confidential Information already knew; (b) becomes public through no fault of the recipient; (c) was independently developed by the recipient; or (d) was rightfully given to the recipient by another party.

- 11. **Termination**

11.1 **Termination in General.**

a. **Termination for Breach.** Either party may suspend performance and/or terminate this Agreement, (including all Order Pages entered into under it) with immediate effect, if the other party: (i) is in material breach of this Agreement where the breach is incapable of remedy; (ii) is in material breach of this Agreement two times or more notwithstanding any remedy of such breach; or (iii) is in material breach of this Agreement where the breach is capable of remedy and fails to remedy that breach within thirty days after receiving written notice of such breach.

b. **Termination for Insolvency.** Either party may suspend performance and/or terminate this Agreement (including all Order Pages entered into under it) with immediate effect, if: (i) the other party enters into an arrangement or composition with or for the benefit of its creditors, goes into administration, receivership or administrative receivership, is declared bankrupt or insolvent or is dissolved or otherwise ceases to carry on business; or (ii) any analogous event happens to the other party in any jurisdiction in which it is incorporated or resident or in which it carries on business or has assets.

11.4 **Effects of Termination.** If this Agreement (including all Order Pages) terminates or expires, then: (i) the rights granted by one party to the other will cease immediately; (ii) Google will provide Customer access to, and the ability to export, the Customer Data for a commercially reasonable period of time at Google's then-current rates for the applicable Services; (iii) after a commercially reasonable period of time, Google will delete Customer Data by removing pointers to it on Google's active and replication servers and overwriting it over time; and (iv) upon request each party will promptly use reasonable endeavours to return or destroy all other Confidential Information of the other party.

- 13. **Limitation of Liability.**

13.1 Nothing in this Agreement shall exclude or limit either party's liability for: (a) death or personal injury resulting from the negligence of either party or their servants, agents or employees; (b) fraud or fraudulent misrepresentation; (c) breach of any implied condition as to title or quiet enjoyment; or (d) misuse of confidential information.

13.2 Save to the extent that this Agreement expressly states otherwise, nothing in this Agreement shall exclude or limit either party's liability under Clause 12 (Indemnification).

13.3 Subject to Clauses 13.1 and 13.2, neither party shall be liable under this Agreement (whether in contract, tort (including negligence) or otherwise) for any of the following losses suffered or incurred by the other party (whether or not such losses were within the contemplation of the parties at the date of this Agreement):

a. loss of actual or anticipated profits (including loss of profits on contracts);

b. loss of anticipated savings;

c. loss of business opportunity;

d. loss of reputation or damage to goodwill; and

e. special, indirect or consequential losses.

13.4 Subject to Clauses 13.1, 13.2 and 13.3, each party's liability under this Agreement (whether in contract, tort (including negligence) or otherwise) for all causes of action arising in any Contract Year shall be limited to the greater of: (a) 125% of the total amount paid and payable by Customer under this Agreement in that Contract Year; or (b) £50,000.

- 15. **Definitions.**

15.1 In this Agreement unless expressly stated otherwise:

"**Acceptable Use Policy**" means the acceptable use policy as may be updated from time to time for the Services located at: https://www.google.com/apps/intl/en/terms/use_policy.html or such other URL as may be provided by Google.

"**Additional Products**" means products, services and applications (whether made available by Google or a third party) that are not part of the Services.

"**Admin Account**" means the administrative account provided to Customer by Google for the purpose of administering the End User Accounts. The use of the Admin Account requires a password, which Google will provide to Customer.

"**Admin Console**" means the online tool provided by Google to Customer for use in reporting and certain other administration functions.

"**Admin Manager**" means the Google business person working with Customer regarding Customer's purchase of the Services.

"**Admin Tool**" means online tools or APIs, or both, provided by Google to Customer to be used by Customer in connection with Customer's administration of the Services for End Users, which may include, among other things, account maintenance and enforcement of Customer usage policies.

"**Administrators**" mean the Customer-designated technical personnel who administer the Services for End Users on Customer's behalf.

"**Ads**" means online advertisements displayed by Google to End Users.

"**Annual Plan**" means a billing option that commits the Customer to purchasing the Services from Google for an annual term.

"**APIs**" means the Google APIs from time to time listed at here: https://developers.google.com/google-apps/app-apis or such other URL as may be provided by Google.

"**API Terms of Use**" means the terms of use as may be updated from time to time located at: https://www.google.com/a/help/intl/en/admins/api_terms.html or such other URL as may be provided by Google.

"**Audit Report**" has the meaning given in Clause 2.9.

"**Brand Features**" means each party's trade names, trademarks, logos, domain names and other distinctive brand features.

"**Confidential Information**" means information disclosed by one party to the other party under this Agreement that is marked as confidential or, from its nature, content or the circumstances in which it is disclosed, might reasonably be supposed to be confidential.

"**Contract Year**" means a period of one year starting on the Effective Date or the relevant anniversary of the Effective Date (as appropriate).

"**Customer Data**" means data (including personal data) provided, generated, transmitted or displayed via the Services by Customer, its Group Companies or End Users.

"**Customer Domain Name(s)**" mean the domain name(s) owned or controlled by Customer, which will be used in connection with the Services and specified on the Order Page.

"**Data Protection Legislation**" means the national provisions adopted pursuant to the EU Directive, in the country in which the Customer is established.

"**Emergency Security Issue**" means either: (a) an End User's use of the Services in violation of the Acceptable Use Policy, which could disrupt: (i) the Services; (ii) other End Users' use of the Services; or (iii) the Google network or servers used to provide the Services; or (b) unauthorized third party access to the Services.

"**End Users**" means the individuals Customer permits to use the Services.

"**End User Account**" means Google-hosted account established by Customer through the Services for an End User.

"**EU Directive**" means Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.

"**Export Control Laws**" means all applicable export and re-export control laws and regulations, including (i) the Export Administration Regulations ("EAR") maintained by the U.S. Department of Commerce, (ii) trade and economic sanctions maintained by the U.S. Treasury Department's Office of Foreign Assets Control, and (iii) the International Traffic in Arms Regulations ("ITAR") maintained by the U.S. Department of State.

"**Fees**" means the amounts charged to Customer by Google for the Services.

"**Google Apps Core Services**" means the services (e.g. Google Apps for Work and Google Apps Vault) specified in the Order Page which are more fully described at: https://www.google.com/a/help/intl/en/users/user_features.html, or such other URL as Google may provide.

"**Google Group**" means those Google Group Companies that may be used to provide the Services to Customer.

"**Group Company**" means in relation to each of the parties: (a) any parent company of that party; and (b) any corporate body of which that party directly or indirectly has control or which is directly or indirectly controlled by the same person or group of persons as that party.

"**Help Centre**" means the Google help centre accessible at https://www.google.com/support/?hl=en or such other URL as may be provided by Google.

"**High Risk Activities**" means uses such as the operation of nuclear facilities, air traffic control, or life support systems, where the use or failure of the Services could lead to death, personal injury, or environmental damage.

"**Initial Services Term**" means, for an Annual Plan, the term for the applicable Services beginning on the Service Commencement Date and continuing for 12 months (or, if different, the duration set forth on the Order Page).

"**Instructions**" means instructions provided by Customer via the Admin Console, instructions initiated by the Customer and End Users in their use of the Services, the written instructions of the Customer specified in this Agreement (as amended or replaced) and any subsequent written instructions from the Customer to Google and acknowledged by Google.

"**Intellectual Property Rights**" means all copyright, moral rights, patent rights, trade marks, design right, rights in or relating to databases, rights in or relating to confidential information, rights in relation to domain names, and any other intellectual property rights (registered or unregistered) throughout the world.

"**Non-Google Apps Products**" means Google products that are not part of the Services, but that may be accessed by End Users using their End User Account login and password. The Non-Google Apps Products are those set forth from time to time at: https://www.google.com/support/a/bin/answer.py?hl=en&answer=181865, or such other URL as Google may provide.

"**Non-Google Apps Product Terms**" means the then-current terms found at the: "https://www.google.com/apps/intl/en/terms/additional_services.html", or such other URL as Google may provide.

"**Notification Email Address**" means the email address designated by Customer to receive email notifications from Google. Customer may change this email address through the Admin Console.

"**Order Page**" means the online order page or pages, or other ordering document acceptable to Google under this Agreement, that Customer completes in signing up for the Services, and that may include: (i) the Services being ordered (including applicable billing and renewal terms); (ii) the Fees; (iii) the number of, and Initial Services Term for, End User Accounts; (iv) the applicable form of payment; and (v) the Customer Domain Name(s).

"**Renewal Term**" means, for an Annual Plan, a renewal term of 12 months.

"**Safe Harbor Privacy Principles**" means the U.S. Department of Commerce Safe Harbor framework requirements as set out at the following URL: http://export.gov/safeharbor/eu/eg_main_018475.asp, or any replacement framework or URL from time to time.

"**Security Incident**" means accidental or unlawful distribution or accidental loss, alteration, or unauthorised disclosure or access to Customer Data by Google, its Subprocessors or any third party, provided that such incident is not directly or indirectly caused by Customer's or End User's act or omission.

"**Services**" means the applicable Google Apps Core Services (e.g. Google Apps Premier Edition or Google Apps for Work and Google Apps Vault) provided by Google and used by Customer under this Agreement. The Services are as described at www.google.com/apps/intl/en/terms/user_features.html or such other URL as Google may provide.

"**Service Commencement Date**" is the date upon which Google makes the Services available to Customer, and will be within one week of Google's receipt of a completed Order Page, unless otherwise agreed by the parties.

"**Service Pages**" mean the web pages displaying the Services to End Users.

"**Services Term**" means the Initial Services Term or the relevant Renewal Term; as applicable.

"**SLA**" means the Service Level Agreement located at https://www.google.com/a/help/intl/en/admins/sla.html, or such other URL as Google may provide.

"**Subprocessors**" means those Google Group Companies and Third Party Suppliers that have logical access to, and process, Customer Data.

"**Suspend**" or "Suspension" means the immediate disabling of access to the Services, or components of the Services, as applicable, to prevent further use of the Services.

"**Taxes**" means any taxes, including sales, use, personal property, value-added, excise, customs fees, import duties or stamp duties or other taxes and duties imposed by governmental agencies of whatever kind and imposed with respect to all transactions under the Agreement, including penalties and interest, but specifically excluding taxes based upon Google's net income.

"**Term**" means:

(1) for an Annual Plan, the Initial Services Term and all Renewal Terms; and

(2) for the Monthly Plan, the period beginning on the Service Commencement Date and continuing for as long as Customer is receiving the Services.

"**Third Party Products**" means any products, software or services not licensed or provided to Customer by Google pursuant to this Agreement.

"**Third Party Request**" means a request from a third party for records relating to an End User's use of the Services. Third Party Requests can be a lawful search warrant, court order, subpoena, other valid legal order, or written consent from the End User permitting the disclosure.

"**Third Party Suppliers**" means the third party suppliers engaged by the Google Group for the purposes of processing Customer Data in the context of the provision of the Services. Additional information about Third Party Suppliers is available at www.google.com/intl/en/work/apps/terms/subprocessors.html, as such information and URL may be updated from time to time by Google. The information available at the URL is accurate at the time of publication.

"**Trademark Guidelines**" means Google's Guidelines for Third Party Use of Google Brand Features as may be updated from time to time located at: https://www.google.co.uk/permissions/guidelines.html, or such other URL as may be provided by Google.

"**TSS Guidelines**" means Google's technical support services guidelines then in effect for the applicable Services, located at:

www.google.com/a/help/intl/en/admins/tssg.html or such other URL as may be provided by Google.

"**URL Terms**" means the Acceptable Use Policy, the SLA and the TSS Guidelines.

15.2 In this Agreement, the words "include" and "including" will not limit the generality of any words preceding them.

Příloha 2 – Data Processing Amendment

The Customer agreeing to these terms ("**Customer**") and Google Inc., Google Ireland Limited, Google Commerce Limited or Google Asia Pacific Pte. Ltd. (as applicable, "**Google**") have entered into a Google Apps for Work Agreement, Google Apps Enterprise Agreement, Google Apps for Business Agreement, Google Apps for Work via Reseller Agreement, Google Apps Enterprise via Reseller Agreement, Google Apps for Business via Reseller Agreement, Google Apps for Education Agreement or Google Apps for Education via Reseller Agreement, as applicable (as amended to date, the "**Google Apps Agreement**"). This amendment (the "**Data Processing Amendment**") is entered into by Customer and Google as of the Amendment Effective Date and amends the Google Apps Agreement.

The "**Amendment Effective Date**" is: (a) if this Data Processing Amendment is incorporated into the Google Apps Agreement by reference, the effective date of the Google Apps Agreement, as defined in that agreement; or (b) if this Data Processing Amendment is not incorporated into the Google Apps Agreement by reference, the date Customer accepts this Data Processing Amendment by clicking to accept these terms.

If this Data Processing Amendment is not incorporated into the Google Apps Agreement by reference and you are accepting on behalf of Customer, you represent and warrant that: (i) you have full legal authority to bind your employer, or the applicable entity, to these terms; (ii) you have read and understand these terms; and (iii) you agree, on behalf of the party you represent, to this Data Processing Amendment. If you do not have the legal authority to bind Customer, please do not click the "I Accept" button.

- 1. **Introduction.**

This Data Processing Amendment reflects the parties' agreement with respect to terms governing the processing of Customer Data under the Google Apps Agreement.

- 2. **Definitions.**

2.1. Capitalized terms used but not defined in this Data Processing Amendment have the meanings given in the Google Apps Agreement. In this Data Processing Amendment, unless expressly stated otherwise:

"**Additional Products**" means products, services and applications that are not part of the Services but that may be accessible, via the Admin Console or otherwise, for use with the Services.

"**Advertising**" means online advertisements displayed by Google to End Users, excluding any advertisements Customer expressly chooses to have Google or any Google Affiliate display in connection with the Services under a separate agreement (for example, Google AdSense advertisements implemented by Customer on a website created by Customer using the "Google Sites" functionality within the Services).

"**Affiliate**" means any entity controlling, controlled by, or under common control with a party, where "control" is defined as (a) the ownership of at least fifty percent (50%) of the equity or beneficial interests of the entity; (b) the right to vote for or appoint a majority of the board of directors or other governing body of the entity; or (c) the power to exercise a controlling influence over the management or policies of the entity.

"**Agreement**" means the Google Apps Agreement, as amended by this Data Processing Amendment and as may be further amended from time to time in accordance with the Google Apps Agreement.

"**Customer Data**" means data (which may include personal data and the categories of data referred to in Appendix 1) submitted, stored, sent or received via the Services by Customer, its Affiliates or End Users.

"**Data Incident**" means (a) any unlawful access to Customer Data stored in the Services or systems, equipment or facilities of Google or its Sub-processors, or (b) unauthorized access to such Services, systems, equipment or facilities that results in loss, disclosure or alteration of Customer Data.

"**Data Privacy Officer**" means Google's Data Privacy Officer for Apps.

"**Data Protection Legislation**" means, as applicable: (a) any national provisions adopted pursuant to the Directive that are applicable to Customer and/or any Customer Affiliates as the controller(s) of the Customer Data; and/or (b) the Federal Data Protection Act of 19 June 1992 (Switzerland).

"**Directive**" means Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.

"**EEA**" means the European Economic Area.

"**Google Group**" means those Google Affiliates involved in provision of the Services to Customer.

"**Instructions**" means Customer's written instructions to Google consisting of the Agreement, including instructions to Google to provide the Services and technical support for the Services as set out in the Agreement; instructions given by Customer, its Affiliates and End Users via the Admin Console and otherwise in its and their use of the Services and related technical support services; and any subsequent written instructions given by Customer to Google and acknowledged by Google.

"**Model Contract Clauses**" or "**MCCs**" means the standard contractual clauses (processors) for the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection.

"**Safe Harbor Certification**" means a current certification to the U.S. Department of Commerce Safe Harbor framework requirements as set out at the following URL: http://export.gov/safeharbor/eu/eg_main_018475.asp, or any replacement framework or URL from time to time.

"**Services**" means, for purposes of this Data Processing Amendment, the Google Apps for Work Services which are described at www.google.com/apps/intl/en/terms/user_features.html (as such services and URL link may be updated or modified by Google from time to time in accordance with the Google Apps Agreement).

"**Subprocessors**" means (a) all Google Group entities that have logical access to and process Customer Data (each, a "**Google Group Subprocessor**"); and (b) all third parties (other than Google Group entities) that are engaged to provide services to Customer and that have logical access to and process Customer Data (each, a "**Third Party Subprocessor**").

"**Term**" means the term of the Google Apps Agreement, as defined in that agreement.

"**Third Party Auditor**" means a qualified and independent third party auditor, whose then-current identity Google will disclose to Customer.

2.2. The terms “personal data”, “processing”, “data subject”, “controller” and “processor” have the meanings given to them in the Directive. The terms “data importer” and “data exporter” have the meanings given to them in the Model Contract Clauses.

- 3. **Term.**

This Data Processing Amendment will take effect on the Amendment Effective Date and, notwithstanding expiry or termination of the Google Apps Agreement, will remain in effect until, and automatically terminate upon, deletion by Google of all data as described in Section 7 (Data Deletion) of this Data Processing Amendment.

- 4. **Data Protection Legislation.**

The parties agree and acknowledge that the Data Protection Legislation may apply to the processing of Customer Data.

- 5. **Processing of Customer Data.**

5.1. **Controller and Processor**. If the Data Protection Legislation applies to the processing of Customer Data, then as between the parties, the parties acknowledge and agree that: (a) Customer is the controller of Customer Data under the Agreement; (b) Google is a processor of such data; (c) Customer will comply with its obligations as a controller under the Data Protection Legislation; and (d) Google will comply with its obligations as a processor under the Agreement. If under the Data Protection Legislation a Customer Affiliate is considered the controller (either alone or jointly with the Customer) with respect to certain Customer Data, Customer represents and warrants to Google that Customer is authorized (i) to give the Instructions to Google and otherwise act on behalf of such Customer Affiliate in relation to such Customer Data as described in this Data Processing Amendment, and (ii) to bind the Customer Affiliate to the terms of this Data Processing Amendment.

5.2. **Scope of Processing**. Google will only process Customer Data in accordance with the Instructions, and will not process Customer Data for any other purpose.

5.3. **Processing Restrictions**. Notwithstanding any other term of the Agreement, Google will not process Customer Data for Advertising purposes or serve Advertising in the Services.

5.4. **Additional Products**. Customer acknowledges that if it installs, uses, or enables Additional Products, the Services may allow such Additional Products to access Customer Data as required for the interoperation of those Additional Products with the Services. This Data Processing Amendment does not apply to the processing of data transmitted to or from such Additional Products. Customer can enable or disable Additional Products. Customer is not required to use Additional Products in order to use the Services.

- 6. **Data Security; Security Compliance; Audits.**

6.1. **Security Measures**. Google will take and implement appropriate technical and organizational measures to protect Customer Data against accidental or unlawful destruction or accidental loss or alteration or unauthorized disclosure or access or other unauthorized processing, as detailed in Appendix 2 ("**Security Measures**"). Google may update or modify the Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services. Customer agrees that it is solely responsible for its use of the Services, including securing its account authentication credentials, and that Google has no obligation to protect Customer Data that Customer elects to store or transfer outside of Google's and its Subprocessors' systems (e.g., offline or on-premise storage).

6.2. **Security Compliance by Google Staff**. Google will take appropriate steps to ensure compliance with the Security Measures by its employees, contractors and Subprocessors to the extent applicable to their scope of performance.

6.3. **Data Incidents**. If Google becomes aware of a Data Incident, Google will promptly notify Customer of the Data Incident, and take reasonable steps to minimize harm and secure Customer Data. Notification(s) of any Data Incident(s) will be delivered to the Notification Email Address provided by Customer in connection with the Agreement or, at Google's discretion, by direct communication (e.g., by phone call or an in-person meeting). Customer acknowledges that it is solely responsible for ensuring the contact information given for purposes of the Notification Email Address is current and valid, and for fulfilling any third party notification obligations. Customer agrees that "Data Incidents" do not include: (i) unsuccessful access attempts or similar events that do not compromise the security or privacy of Customer Data, including pings, port scans, denial of service attacks and other network attacks on firewalls or

networked systems; or (ii) accidental loss or disclosure of Customer Data caused by Customer's use of the Services or Customer's loss of account authentication credentials. Google's obligation to report or respond to a Data Incident under this Section will not be construed as an acknowledgement by Google of any fault or liability with respect to the Data Incident.

6.4. **Compliance with Security and Privacy Standards; SOC 2 and 3 Reports**. During the Term, Google will maintain the following:

(a) its ISO/IEC 27001:2013 Certification or a comparable certification ("**ISO 27001 Certification**") for the Services;

(b) conformity of the Services with ISO/IEC 27018:2014 or a comparable standard ("**ISO 27018 Conformity**"), as independently verified;

(c) its confidential Service Organization Control (SOC) 2 Report (or a comparable report) on Google's systems examining logical security controls, physical security controls, and system availability as related to the Services (the "**SOC 2 Report**"), as produced by the Third Party Auditor and updated at least once every eighteen (18) months; and

(d) its Service Organization Control (SOC) 3 Report (or a comparable report) as related to the Services (the "**SOC 3 Report**"), as produced by the Third Party Auditor and updated at least once every eighteen (18) months.

6.5. **Auditing Security Compliance**

6.5.1. **Reviews of Security Documentation.** Google will make the following available for review by Customer:

(a) the certificate issued in relation to Google's ISO 27001 Certification;

(b) the then-current SOC 3 Report;

(c) a summary or redacted version of the then-current confidential SOC 2 Report; and

(d) following a request by Customer in accordance with Section 6.5.4 below, the then-current confidential SOC 2 Report.

6.5.2. **Customer Audits.** If Customer (or an authorized Customer Affiliate) has entered into Model Contract Clauses as described in Section 10.2 of this Data

Processing Amendment, Customer or such Customer Affiliate may exercise the audit rights granted under clauses 5(f) and 12(2) of such Model Contract Clauses:

(a) by instructing Google to execute the audit as described in Sections 6.4 and 6.5.1 above; and/or

(b) following a request by Customer in accordance with Section 6.5.4 below, by executing an audit as described in such Model Contract Clauses.

- 7. **Data Deletion.**

7.1. **Deletion by Customer and End Users**. During the Term, Google will provide Customer or End Users with the ability to delete Customer Data in a manner consistent with the functionality of the Services and in accordance with the terms of the Agreement. Once Customer or End User deletes Customer Data and such Customer Data cannot be recovered by the Customer or End User, such as from the "trash" ("**Customer-Deleted Data**"), Google will delete such data from its systems as soon as reasonably practicable within a maximum period of 180 days, unless applicable legislation or legal process prevents it from doing so.

7.2. **Deletion on Standard Termination**. On expiry or termination of the Google Apps Agreement (or, if applicable, on expiry of any post-termination period during which Google may agree to continue providing the Services), Google will, subject to Section 7.3 (Deletion on Termination for Non-Payment or No Purchase) below, delete all Customer-Deleted Data from its systems as soon as reasonably practicable within a maximum period of 180 days, unless applicable legislation or legal process prevents it from doing so.

7.3. **Deletion on Termination for Non-Payment or No Purchase**. On termination of the Google Apps Agreement due to Customer breaching its payment obligations or opting not to purchase the Services at the end of a free trial of the Services, Google will delete all Customer Data from its systems within a maximum period of 180 days, unless applicable legislation or legal process prevents it from doing so.

- 8. **Access to Data.**

8.1. **Access; Export of Data**. During the Term, Google will provide Customer with access to and the ability to correct, block and export Customer Data in a manner

consistent with the functionality of the Services and in accordance with the terms of the Agreement. To the extent Customer, in its use and administration of the Services during the Term, does not have the ability to correct or block Customer Data as required by applicable law, or to migrate Customer Data to another system or service provider, Google will comply with any reasonable requests by Customer to assist in facilitating such actions to the extent Google is legally permitted to do so and has reasonable access to the Customer Data.

8.2. **End User Requests**. During the Term, if Google receives any request from an End User for records relating to that End User's personal data included in the Customer Data, Google will advise such End User to submit its request to Customer. Customer will be responsible for responding to any such request using the functionality of the Services.

- 9. **Data Privacy Officer.**

The Data Privacy Officer can be contacted by Customer Administrators at: https://support.google.com/a/contact/gfw_dpo (or via such other means as may be provided by Google). Administrators must be signed in to their Admin Account to use this address.

- 10. **Data Transfers.**

10.1. **Data Storage and Processing Facilities**. Google may store and process Customer Data in the United States or any other country in which Google or any of its Subprocessors maintains facilities, subject to Section 10.2 (Transfers of Data Out of the EEA) below.

10.2. **Transfers of Data Out of the EEA**. If the storage and processing of Customer Data (as set out in Section 10.1 above) involves transfers of Customer personal data out of the EEA and Data Protection Legislation applies to those transfers, Google will:

10.2.1 ensure that Google Inc. maintains its Safe Harbor Certification, and that the transfers are made in accordance with such Safe Harbor Certification; and/or

10.2.2 ensure that Google Inc. as the data importer of such Customer personal data enters into Model Contract Clauses with Customer (or an authorized Customer

Affiliate) as the data exporter of such data, if Customer so requests, and that the transfers are made in accordance with any such Model Contract Clauses; and/or

10.2.3 adopt an alternative solution that achieves compliance with the terms of the Directive for transfers of personal data to a third country, and ensure that the transfers are made in accordance with any such compliance solution.

10.3. **Safe Harbor Certification and Processing Practices**. While Google Inc. maintains its Safe Harbor Certification pursuant to Section 10.2.1, Google will ensure that: (a) the scope of such Safe Harbor Certification includes Customer Data; and (b) the Google Group's processing practices in respect of Customer Data remain consistent with those described in such Safe Harbor Certification.

10.4. **Data Center Information**. Google will make available to Customer information about the countries in which data centers used to store Customer Data are located.

- 11. **Subprocessors.**

11.1. **Subprocessors**. Google may engage Subprocessors to provide parts of the Services and related technical support services, subject to the restrictions in this Data Processing Amendment.

11.2. **Subprocessing Restrictions**. Google will ensure that Subprocessors only access and use Customer Data in accordance with the terms of the Agreement and that Subprocessors are bound by written agreements that require them to provide at least the level of data protection required by the following, as applicable pursuant to Section 10.2 (Transfers of Data Out of the EEA): (a) any Safe Harbor Certification maintained by Google Inc.; (b) any Model Contract Clauses entered into by Google Inc. and Customer (or an authorized Customer Affiliate); and/or (c) any alternative compliance solution adopted by Google.

11.3. **Consent to Subprocessing**. Customer consents to Google subcontracting the processing of Customer Data to Subprocessors in accordance with the Agreement. If the Model Contract Clauses have been entered into as described above, Customer (or, if applicable, an authorized Customer Affiliate) consents to Google Inc. subcontracting the processing of Customer Data in accordance with the terms of the Model Contract Clauses.

- 14. **Effect of Amendment.**

To the extent of any conflict or inconsistency between the terms of this Data Processing Amendment and the remainder of the Agreement, the terms of this Data Processing Amendment will govern. Subject to the amendments in this Data Processing Amendment, the Agreement remains in full force and effect.

Appendix 1: Categories of Data and Data Subjects

Categories of Data

Personal data submitted, stored, sent or received by Customer or End Users via the Services may include the following categories of data: user IDs, email, documents, presentations, images, calendar entries, tasks and other electronic data

Data Subjects

Personal data submitted, stored, sent or received via the Services may concern the following categories of data subjects: End Users including Customer's employees and contractors; the personnel of Customer's customers, suppliers and subcontractors; and any other person who transmits data via the Services, including individuals collaborating and communicating with End Users.

Appendix 2: Security Measures

As of the Amendment Effective Date, Google will take and implement the Security Measures set out in this Appendix to the Data Processing Amendment. Google may update or modify such Security Measures from time to time provided that such updates and modifications do not result in the degradation of the overall security of the Services.

- 1. **Data Center & Network Security.**
  - (a) **Data Centers.**
    - **Infrastructure**. Google maintains geographically distributed data centers. Google stores all production data in physically secure data centers.
    - **Redundancy**. Infrastructure systems have been designed to eliminate single points of failure and minimize the impact of anticipated environmental risks. Dual circuits, switches, networks or other necessary devices help provide this redundancy. The Services are designed to allow Google to perform certain types of preventative and corrective maintenance without interruption. All environmental equipment and facilities have documented

preventative maintenance procedures that detail the process for and frequency of performance in accordance with the manufacturer's or internal specifications. Preventative and corrective maintenance of the data center equipment is scheduled through a standard change process according to documented procedures.

- **Power**. The data center electrical power systems are designed to be redundant and maintainable without impact to continuous operations, 24 hours a day, and 7 days a week. In most cases, a primary as well as an alternate power source, each with equal capacity, is provided for critical infrastructure components in the data center. Backup power is provided by various mechanisms such as uninterruptible power supplies (UPS) batteries, which supply consistently reliable power protection during utility brownouts, blackouts, over voltage, under voltage, and out-of-tolerance frequency conditions. If utility power is interrupted, backup power is designed to provide transitory power to the data center, at full capacity, for up to 10 minutes until the diesel generator systems take over. The diesel generators are capable of automatically starting up within seconds to provide enough emergency electrical power to run the data center at full capacity typically for a period of days.
- **Server Operating Systems**. Google servers use a Linux based implementation customized for the application environment. Data is stored using proprietary algorithms to augment data security and redundancy. Google employs a code review process to increase the security of the code used to provide the Services and enhance the security products in production environments.
- **Businesses Continuity**. Google replicates data over multiple systems to help to protect against accidental destruction or loss. Google has designed and regularly plans and tests its business continuity planning/disaster recovery programs.

- (b) **Networks & Transmission.**
  - **Data Transmission**. Data centers are typically connected via high-speed private links to provide secure and fast data transfer between data centers. This is designed to prevent data from being read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media. Google transfers data via Internet standard protocols.
  - **External Attack Surface**. Google employs multiple layers of network devices and intrusion detection to protect its external attack surface. Google considers potential attack vectors and incorporates appropriate purpose built technologies into external facing systems.
  - **Intrusion Detection**. Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. Google's intrusion detection involves:
    - 1. Tightly controlling the size and make-up of Google's attack surface through preventative measures;
    - 2. Employing intelligent detection controls at data entry points; and
    - 3. Employing technologies that automatically remedy certain dangerous situations.
  - **Incident Response**. Google monitors a variety of communication channels for security incidents, and Google's security personnel will react promptly to known incidents.
  - **Encryption Technologies**. Google makes HTTPS encryption (also referred to as SSL or TLS connection) available.

- 2. **Access and Site Controls.**
  - (a) **Site Controls.**
    - **On-site Data Center Security Operation**. Google's data centers maintain an on-site security operation responsible for all physical

data center security functions 24 hours a day, 7 days a week. The on-site security operation personnel monitor Closed Circuit TV (CCTV) cameras and all alarm systems. On-site Security operation personnel perform internal and external patrols of the data center regularly.

- **Data Center Access Procedures**. Google maintains formal access procedures for allowing physical access to the data centers. The data centers are housed in facilities that require electronic card key access, with alarms that are linked to the on-site security operation. All entrants to the data center are required to identify themselves as well as show proof of identity to on-site security operations. Only authorized employees, contractors and visitors are allowed entry to the data centers. Only authorized employees and contractors are permitted to request electronic card key access to these facilities. Data center electronic card key access requests must be made through e-mail, and require the approval of the requestor's manager and the data center director. All other entrants requiring temporary data center access must: (i) obtain approval in advance from the data center managers for the specific data center and internal areas they wish to visit; (ii) sign in at on-site security operations; and (iii) reference an approved data center access record identifying the individual as approved.
- **On-site Data Center Security Devices**. Google's data centers employ an electronic card key and biometric access control system that is linked to a system alarm. The access control system monitors and records each individual's electronic card key and when they access perimeter doors, shipping and receiving, and other critical areas. Unauthorized activity and failed access attempts are logged by the access control system and investigated, as appropriate. Authorized access throughout the business operations and data centers is restricted based on zones and the individual's job responsibilities. The fire doors at

the data centers are alarmed. CCTV cameras are in operation both inside and outside the data centers. The positioning of the cameras has been designed to cover strategic areas including, among others, the perimeter, doors to the data center building, and shipping/receiving. On-site security operations personnel manage the CCTV monitoring, recording and control equipment. Secure cables throughout the data centers connect the CCTV equipment. Cameras record on site via digital video recorders 24 hours a day, 7 days a week. The surveillance records are retained for up to 30 days based on activity.

- (b) **Access Control.**
  - **Infrastructure Security Personnel**. Google has, and maintains, a security policy for its personnel, and requires security training as part of the training package for its personnel. Google's infrastructure security personnel are responsible for the ongoing monitoring of Google's security infrastructure, the review of the Services, and responding to security incidents.
  - **Access Control and Privilege Management**. Customer's Administrators and End Users must authenticate themselves via a central authentication system or via a single sign on system in order to use the Services. Each application checks credentials in order to allow the display of data to an authorized End User or authorized Administrator.
  - **Internal Data Access Processes and Policies – Access Policy**. Google's internal data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process personal data. Google aims to design its systems to: (i) only allow authorized persons to access data they are authorized to access; and (ii) ensure that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording. The systems are designed to detect any inappropriate access. Google

employs a centralized access management system to control personnel access to production servers, and only provides access to a limited number of authorized personnel. LDAP, Kerberos and a proprietary system utilizing RSA keys are designed to provide Google with secure and flexible access mechanisms. These mechanisms are designed to grant only approved access rights to site hosts, logs, data and configuration information. Google requires the use of unique user IDs, strong passwords, two factor authentication and carefully monitored access lists to minimize the potential for unauthorized account use. The granting or modification of access rights is based on: the authorized personnel's job responsibilities; job duty requirements necessary to perform authorized tasks; and a need to know basis. The granting or modification of access rights must also be in accordance with Google's internal data access policies and training. Approvals are managed by workflow tools that maintain audit records of all changes. Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication (e.g., login to workstations), password policies that follow at least industry standard practices are implemented. These standards include password expiry, restrictions on password reuse and sufficient password strength. For access to extremely sensitive information (e.g., credit card data), Google uses hardware tokens.

- 3. **Data.**
  - (a) **Data Storage, Isolation & Authentication**.
  - Google stores data in a multi-tenant environment on Google-owned servers. Data, the Services database and file system architecture are replicated between multiple geographically dispersed data centers. Google logically isolates data on a per End User basis at the application layer. Google logically isolates each Customer's data, and logically separates each End User's data from the data of other End Users, and

data for an authenticated End User will not be displayed to another End User (unless the former End User or an Administrator allows the data to be shared). A central authentication system is used across all Services to increase uniform security of data.

- The Customer will be given control over specific data sharing policies. Those policies, in accordance with the functionality of the Services, will enable Customer to determine the product sharing settings applicable to End Users for specific purposes. Customer may choose to make use of certain logging capability that Google may make available via the Services, products and APIs. Customer agrees that its use of the APIs is subject to the API Terms of Use. Google agrees that changes to the APIs will not result in the degradation of the overall security of the Services.
- (b) **Decommissioned Disks and Disk Erase Policy**.
- Certain disks containing data may experience performance issues, errors or hardware failure that lead them to be decommissioned ("Decommissioned Disk"). Every Decommissioned Disk is subject to a series of data destruction processes (the "Disk Erase Policy") before leaving Google's premises either for reuse or destruction. Decommissioned Disks are erased in a multi-step process and verified complete by at least two independent validators. The erase results are logged by the Decommissioned Disk's serial number for tracking. Finally, the erased Decommissioned Disk is released to inventory for reuse and redeployment. If, due to hardware failure, the Decommissioned Disk cannot be erased, it is securely stored until it can be destroyed. Each facility is audited regularly to monitor compliance with the Disk Erase Policy

- 4. **Personnel Security.**
  - Google personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. Google conducts reasonably appropriate backgrounds checks to the extent

legally permissible and in accordance with applicable local labor law and statutory regulations.

- Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, Google's confidentiality and privacy policies. Personnel are provided with security training. Personnel handling Customer Data are required to complete additional requirements appropriate to their role (eg., certifications). Google's personnel will not process Customer Data without authorization.

- 5. **Subprocessor Security.**

Prior to onboarding Subprocessors, Google conducts an audit of the security and privacy practices of Subprocessors to ensure Subprocessors provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Google has assessed the risks presented by the Subprocessor, then subject always to the requirements set out in Section 11.2 (Subprocessing Restrictions) of this Data Processing Amendment, the Subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms.

Příloha 3 – Microsoft Online Subscription Agreement

This Microsoft Online Subscription Agreement is between the entity you represent, or, if you do not designate an entity in connection with a Subscription purchase or renewal, you individually ("you" or "your"), and Microsoft Corporation ("Microsoft", "we", "us", or "our"). It consists of the terms and conditions below, as well as the Online Services Terms, the SLAs, and the Offer Details for your Subscription or renewal (together, the "agreement"). It is effective on the date we provide you with confirmation of your Subscription or the date on which your Subscription is renewed as applicable. Key terms are defined in Section 9.

1. Use of Online Services.

d. Customer Data. You are solely responsible for the content of all Customer Data. You will secure and maintain all rights in Customer Data necessary for us to provide the Online Services to you without violating the rights of any third party or otherwise obligating Microsoft to you or to any third party. Microsoft does not and will not assume any obligations with respect to Customer Data or to your use of the Product other than as expressly set forth in this Agreement or as required by applicable law

3. Term, termination, and suspension.

a. Agreement term and termination. This agreement will remain in effect until the expiration, termination, or renewal of your Subscription, whichever is earliest.

4. Warranties.

a. Limited warranty.

(i) Online Services. We warrant that the Online Services will meet the terms of the SLA during the Term. Your only remedies for breach of this warranty are those in the SLA.

(ii) Software. We warrant for one year from the date you first use the Software that it will perform substantially as described in the applicable user documentation. If Software fails to meet this warranty we will, at our option and as your exclusive remedy, either (1) return the price paid for the Software or (2) repair or replace the Software.

b. Limited warranty exclusions. This limited warranty is subject to the following limitations:

(i) any implied warranties, guarantees or conditions not able to be disclaimed as a matter of law will last one year from the start of the limited warranty;

(ii) this limited warranty does not cover problems caused by accident, abuse or use of the Products in a manner inconsistent with this agreement or our published documentation or guidance, or resulting from events beyond our reasonable control;

(iii) this limited warranty does not apply to problems caused by a failure to meet minimum system requirements; and

(iv) this limited warranty does not apply to Previews or Limited Offerings.

c. DISCLAIMER. Other than this warranty, we provide no warranties, whether express, implied, statutory, or otherwise, including warranties of merchantability or fitness for a particular purpose. These disclaimers will apply except to the extent applicable law does not permit them.

5. Defense of claims.

a. Defense.

(i) We will defend you against any claims made by an unaffiliated third party that a Product infringes that third party's patent, copyright or trademark or makes unlawful use of its trade secret.

(ii) You will defend us against any claims made by an unaffiliated third party that (1) any Customer Data, Customer Solution, or Non-Microsoft Products, or services you provide, directly or indirectly, in using a Product infringes the third party's patent, copyright, or trademark or makes unlawful use of its trade secret; or (2) arises from violation of the Acceptable Use Policy.

b. Limitations. Our obligations in Section 5a won't apply to a claim or award based on: (i) any Customer Solution, Customer Data, Non-Microsoft Products, modifications you make to the Product, or services or materials you provide or make available as part of using the Product; (ii) your combination of the Product with, or damages based upon the value of, Customer Data, or a Non-Microsoft Product, data, or business process; (iii) your use of a Microsoft trademark without our express written consent, or your use of the Product after

we notify you to stop due to a third-party claim; (iv) your redistribution of the Product to, or use for the benefit of, any unaffiliated third party; or (v) Products provided free of charge.

c. Remedies. If we reasonably believe that a claim under Section 5.a.(i) may bar your use of the Product, we will seek to: (i) obtain the right for you to keep using it; or (ii) modify or replace it with a functional equivalent and notify you to stop use of the prior version of the Product. If these options are not commercially reasonable, we may terminate your rights to use the Product and then refund any advance payments for unused Subscription rights.

d. Obligations. Each party must notify the other promptly of a claim under this Section. The party seeking protection must (i) give the other sole control over the defense and settlement of the claim; and (ii) give reasonable help in defending the claim. The party providing the protection will (1) reimburse the other for reasonable out-of-pocket expenses that it incurs in giving that help and (2) pay the amount of any resulting adverse final judgment or settlement. The parties' respective rights to defense and payment of judgments (or settlement the other consents to) under this Section 5 are in lieu of any common law or statutory indemnification rights or analogous rights, and each party waives such common law or statutory rights.

6. Limitation of liability.

a. Limitation. The aggregate liability of each party for all claims under this agreement is limited to direct damages up to the amount paid under this agreement for the Online Service during the 12 months before the cause of action arose; provided, that in no event will a party's aggregate liability for any Online Service exceed the amount paid for that Online Service during the Subscription. For Products provided free of charge, Microsoft's liability is limited to direct damages up to $5,000.00 USD.

b. EXCLUSION. Neither party will be liable for loss of revenue or indirect, special, incidental, consequential, punitive, or exemplary damages, or damages for lost profits, revenues, business interruption, or loss of business information, even if the party knew they were possible or reasonably foreseeable.

c. Exceptions to limitations. The limits of liability in this Section apply to the fullest extent permitted by applicable law, but do not apply to: (1) the parties' obligations under Section 5; or (2) violation of the other's intellectual property rights.

9. Definitions.

Any reference in this agreement to "day" will be a calendar day.

"Acceptable Use Policy" is set forth in the Online Services Terms.

"Affiliate" means any legal entity that a party owns, that owns a party, or that is under common ownership with a party. "Ownership" means, for purposes of this definition, control of more than a 50% interest in an entity.

"Consumption Offering", "Commitment Offering", or "Limited Offering" describe categories of Subscription offers and are defined in Section 2.

"Customer Data" is defined in the Online Services Terms.

"Customer Solution" is defined in the Online Services Terms.

"End User" means any person you permit to access Customer Data hosted in the Online Services or otherwise use the Online Services, or any user of a Customer Solution.

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

"Non-Microsoft Product" is defined in the Online Services Terms.

"Offer Details" means the pricing and related terms applicable to a Subscription offer, as published in the Portal.

"Online Services" means any of the Microsoft-hosted online services subscribed to by Customer under this agreement, including Dynamics CRM Online Services, Office 365 Services, Microsoft Azure Services, or Microsoft Intune Online Services.

"Online Services Terms" means the terms that apply to your use of the Products available at http://www.microsoft.com/licensing/onlineuserights. The Online Services Terms include terms governing your use of Products that are in addition to the terms in this agreement.

"Previews" means preview, beta, or other pre-release version or feature of the Online Services or Software offered by Microsoft to obtain customer feedback.

"Portal" means the Online Services' respective web sites that can be found at http://www.microsoft.com/licensing/online-services/default.aspx, http://azure.microsoft.com/en-us/pricing/, or at an alternate website we identify.

"Product" means any Online Service (including any Software).

"SLA" means the commitments we make regarding delivery and/or performance of an Online Service, as published at http://www.microsoftvolumelicensing.com/csla, http://azure.microsoft.com/en-us/support/legal/sla/, or at an alternate site that we identify.

"Software" means software we provide for installation on your device as part of your Subscription or to use with the Online Service to enable certain functionality.

"Subscription" means an enrollment for Online Services for a defined Term as specified on the Portal. You may purchase multiple Subscriptions, which may be administered separately and which will be governed by the terms of a separate Microsoft Online Subscription Agreement.

Příloha 4 – (Microsoft) Online Services Terms, srpen 2016, vybraná část

General Terms

Customer may use the Online Services and related software as expressly permitted in Customer's volume licensing agreement. Microsoft reserves all other rights. Customer must acquire and assign the appropriate subscription licenses required for its use of each Online Service. Each user that accesses the Online Service must be assigned a User SL or access the Online Service only through a device that has been assigned a Device SL, unless specified otherwise in the Online Service-specific Terms. Attachment 2 describes SL Suites that also fulfill requirements for User SLs. Customer has no right to use an Online Service after the SL for that Online Service ends.

Definitions

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

"Customer Data" means all data, including all text, sound, video, or image files, and software, that are provided to Microsoft by, or on behalf of, Customer through use of the Online Service.

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

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

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

"Non-Microsoft Product" means any third-party-branded software, data, service, website or product.

"Online Service" means a Microsoft-hosted service to which Customer subscribes under a Microsoft volume licensing agreement, including any service identified in the Online Services section of the Product Terms. The Product Terms is located at http://go.microsoft.com/?linkid=9839207.

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

"SL" means subscription license.

Data Retention

At all times during the term of Customer's subscription, Customer will have the ability to access and extract Customer Data stored in each Online Service. Except for free trials, Microsoft will retain Customer Data stored in the Online Service in a limited function account for 90 days after expiration or termination of Customer's subscription so that Customer may extract the data. After the 90-day retention period ends, Microsoft will disable Customer's account and delete the Customer Data.

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

Validation, Automatic Updates, and Collection for Software

Microsoft may automatically check the version of any of its software. Devices on which the software is installed may periodically provide information to enable

Microsoft to verify that the software is properly licensed. This information includes the software version, the end user's user account, product ID information, a machine ID, and the internet protocol address of the device. If the software is not properly licensed, its functionality will be affected. Customer may only obtain updates or upgrades for the software from Microsoft or authorized sources. By using the software, Customer consents to the transmission of the information described in this section. Microsoft may recommend or download to Customer's devices updates or supplements to this software, with or without notice. Some Online Services may require, or may be enhanced by, the installation of local software (e.g., agents, device management applications) ("Apps"). The Apps may collect data about the use and performance of the Apps, which may be transmitted to Microsoft and used for the purposes described in this OST.

Third-party Software Components

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

General Privacy and Security Terms

Scope

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

Use of Customer Data

Customer Data will be used only to provide Customer the Online Services including purposes compatible with providing those services. Microsoft will not use Customer Data or derive information from it for any advertising or similar commercial purposes. As between the parties, Customer retains all right, title and interest in and to Customer Data. Microsoft acquires no rights in Customer Data, other than the rights Customer

grants to Microsoft to provide the Online Services to Customer. This paragraph does not affect Microsoft's rights in software or services Microsoft licenses to Customer.

Disclosure of Customer Data

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

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

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

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

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

Security

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

Security Incident Notification

If Microsoft becomes aware of any unlawful access to any Customer Data stored on Microsoft's equipment or in Microsoft's facilities, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of Customer Data (each a "Security Incident"), Microsoft will promptly (1) notify Customer of the Security Incident; (2) investigate the Security Incident and provide Customer with detailed information about the Security Incident; and (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

Notification(s) of Security Incidents will be delivered to one or more of Customer's administrators by any means Microsoft selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information on each applicable Online Services portal. Microsoft's obligation to report or respond to a Security Incident under this section is not an acknowledgement by Microsoft of any fault or liability with respect to the Security Incident.

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

Location of Data Processing

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

Preview Releases

Microsoft may offer preview, beta or other pre-release features, data center locations, and services ("Previews") for optional evaluation. Previews may employ lesser or different privacy and security measures than those typically present in the Online

Services. Unless otherwise provided, Previews are not included in the SLA for the corresponding Online Service.

Use of Subcontractors

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

Data Processing Terms

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

The Data Processing Terms also include the "Standard Contractual Clauses," pursuant to the European Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under the EU Data Protection Directive. The Standard Contractual Clauses are in Attachment 3. In addition,

- Execution of the volume licensing agreement includes execution of Attachment 3, which is countersigned by Microsoft Corporation;
- The terms in Customer's volume licensing agreement, including the DPT, constitute a data processing agreement under which Microsoft is the data processor; and
- The DPT control over any inconsistent or conflicting provision in Customer's volume licensing agreement and, for each subscription, will remain in full force and effect until all of the related Customer Data is deleted from Microsoft's systems in accordance with the DPT.

Customer may opt out of the "Standard Contractual Clauses" or the Data Processing Terms in their entirety. To opt out, Customer must send the following information to

Microsoft in a written notice (under terms of the Customer's volume licensing agreement):

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

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

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

Online Services	
Microsoft Dynamics Online Services	The following services: Microsoft Dynamics CRM Online, Microsoft Dynamics Marketing, and Microsoft Social Engagement. Microsoft Dynamics Online Services do not include (1) Microsoft Dynamics CRM for supported devices, which includes but is not limited to Microsoft Dynamics CRM Online services for tablets and/or smartphones; or (2) any other separately-branded service made available with or connected to Microsoft Dynamics CRM Online, Microsoft Dynamics Marketing, or Microsoft Social Engagement.

Online Services	
Office 365 Services	The following services, each as a standalone service or as included in an Office 365-branded plan or suite: Exchange Online, Exchange Online Archiving, Exchange Online Protection, Office 365 Advanced Threat Protection, SharePoint Online, OneDrive for Business, Project Online, Skype for Business Online, Sway, Office Online, Delve Analytics, Customer Lockbox, and Yammer Enterprise. Office 365 Services do not include Office 365 ProPlus, any portion of PSTN Services that operate outside of Microsoft's control, any client software, or any separately branded service made available with an Office 365-branded plan or suite, such as a Bing or a service branded "for Office 365."
Microsoft Azure Core Services	Active Directory, API Management, App Services (API Apps, Mobile Apps, Web Apps, Automation, Backup, Batch, BizTalk Services, Cloud Services, DocumentDB, Event Hubs, Express Route, HDInsight, Key Vault, Load Balancer, Machine Learning, Management Portal, Media Services, Multi-Factor Authentication, Notification Hub, Operational Insights, Redis Cache, RemoteApp, Rights Management Service, Scheduler, Service Bus, Site Recovery, SQL Database, Storage, StorSimple, Stream Analytics, Traffic Manager, Virtual Machines, Virtual Network, Visual Studio Team Services, and Workflow Manager.
Microsoft Intune Online Services	The cloud service portion of Microsoft Intune such as the Microsoft Intune Add-on Product or a management service provided by Microsoft Intune such as Mobile Device Management for Office 365.
Microsoft Power BI	The cloud service portion of Microsoft Power BI offered

Online Services	
Services	as a standalone service or as included in an Office 365-branded plan or suite, but excluding data catalog functionality, the Power BI mobile applications, or Power BI Desktop.

Location of Customer Data at Rest

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

- **Office 365 Services.** If Customer provisions its tenant in Australia, the European Union, India, Japan or the United States (each of the foregoing a Geo), Microsoft will store the following Customer Data at rest only within that Geo: (1) Exchange Online mailbox content (e-mail body, calendar entries, and the content of e-mail attachments) and (2) SharePoint Online site content and the files stored within that site.

Privacy

- **Customer Data Deletion or Return**. No more than 180 days after expiration or termination of Customer's use of an Online Service, Microsoft will disable the account and delete Customer Data from the account.

- **Transfer of Customer Data**. Unless Customer has opted out of the Standard Contractual Clauses, all transfers of Customer Data out of the European Union, European Economic Area, and Switzerland shall be governed by the Standard Contractual Clauses. Microsoft 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.

- **Microsoft Personnel**. Microsoft personnel will not process Customer Data without authorization from Customer. Microsoft personnel are obligated to maintain the security and secrecy of any Customer Data as provided in the DPT and this obligation continues even after their engagements end.

- **Subcontractor Transfer**. Microsoft may hire subcontractors to provide certain limited or ancillary services on its behalf. Any subcontractors to whom Microsoft transfers Customer Data, even those used for storage purposes, will have entered into written agreements with Microsoft that are no less protective than the DPT. Customer has previously consented to Microsoft's transfer of Customer Data to subcontractors as described in the DPT. Except as set forth in the DPT, or as Customer may otherwise authorize, Microsoft will not transfer to any third party (not even for storage purposes) personal data Customer provides to Microsoft through the use of the Online Services. Each Online Service has a website that lists subcontractors that are authorized to access Customer Data as well as the limited or ancillary services they provide. At least 14 days before authorizing any new subcontractor to access Customer Data, Microsoft will update the applicable website and provide Customer with a mechanism to obtain notice of that update. If Customer does not approve of a new subcontractor, then Customer may terminate the affected Online Service without penalty by providing, before the end of the notice period, written notice of termination that includes an explanation of the grounds for non-approval. If the affected Online Service is part of a suite (or similar single purchase of services), then any termination will apply to the entire suite. After termination, Microsoft will remove payment obligations for the terminated Online Services from subsequent Customer invoices.

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

Communications and Operations Management	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. **Operational Policy**. Microsoft maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Customer Data. **Data Recovery Procedures** - On an ongoing basis, but in no case less frequently than once a week (unless no Customer Data has been updated during that period), Microsoft maintains multiple copies of Customer Data from which Customer Data can be recovered. - Microsoft stores copies of Customer Data and data recovery procedures in a different place from where the primary computer equipment processing the Customer Data is located. - Microsoft has specific procedures in place governing access to copies of Customer Data. - Microsoft reviews data recovery procedures at least every six months, except for data recovery procedures for Azure Government Services , which are reviewed every twelve months. - Microsoft logs data restoration efforts, including the person responsible, the description of the restored data and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process. **Malicious Software**. Microsoft has anti-malware controls to help avoid malicious software gaining unauthorized access to Customer Data, including malicious software originating from public networks. **Data Beyond Boundaries**

	- Microsoft encrypts, or enables Customer to encrypt, Customer Data that is transmitted over public networks. - Microsoft restricts access to Customer Data in media leaving its facilities. **Event Logging**. Microsoft logs, or enables Customer to log, access and use of information systems containing Customer Data, registering the access ID, time, authorization granted or denied, and relevant activity.
Access Control	**Access Policy**. Microsoft maintains a record of security privileges of individuals having access to Customer Data. **Access Authorization** - Microsoft maintains and updates a record of personnel authorized to access Microsoft systems that contain Customer Data. - Microsoft deactivates authentication credentials that have not been used for a period of time not to exceed six months. - Microsoft identifies those personnel who may grant, alter or cancel authorized access to data and resources. - Microsoft ensures that where more than one individual has access to systems containing Customer Data, the individuals have separate identifiers/log-ins. **Least Privilege** - Technical support personnel are only permitted to have access to Customer Data when needed. - Microsoft restricts access to Customer Data to only those individuals who require such access to perform their job function. **Integrity and Confidentiality** - Microsoft instructs Microsoft personnel to disable administrative sessions when leaving premises Microsoft controls or when computers are otherwise left unattended. - Microsoft stores passwords in a way that makes them unintelligible while they are in force.

	Authentication - Microsoft uses industry standard practices to identify and authenticate users who attempt to access information systems. - Where authentication mechanisms are based on passwords, Microsoft requires that the passwords are renewed regularly. - Where authentication mechanisms are based on passwords, Microsoft requires the password to be at least eight characters long. - 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 unreasonable delay and, in any event, within 30 calendar days. - Microsoft tracks, or enables Customer to track, disclosures of

	Customer Data, including what data has been disclosed, to whom, and at what time. **Service Monitoring**. Microsoft security personnel verify logs at least every six months to propose remediation efforts if necessary.
Business Continuity Management	- Microsoft maintains emergency and contingency plans for the facilities in which Microsoft information systems that process Customer Data are located. - Microsoft's redundant storage and its procedures for recovering data are designed to attempt to reconstruct Customer Data in its original or last-replicated state from before the time it was lost or destroyed.

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

- **End Users in EEA or Switzerland**. Terms used in the DPT that are not specifically defined will have the meaning in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the "EU Data Protection Directive").

- **Intent of the Parties**. For the Online Services, Microsoft is a data processor (or sub-processor) acting on Customer's behalf. As data processor (or sub-processor), Microsoft will only act upon Customer's instructions. The OST and Customer's volume licensing agreement (including the terms and conditions incorporated by reference therein), along with Customer's use and configuration of features in the Online Services, are Customer's complete and final instructions to Microsoft for the processing of Customer Data. Any additional or alternate instructions must be agreed to according to the process for amending Customer's volume licensing agreement.

- **Duration and Object of Data Processing**. The duration of data processing shall be for the term designated under Customer's volume licensing agreement. The objective of the data processing is the performance of the Online Services.

- **Scope and Purpose of Data Processing**. The scope and purpose of processing of Customer Data, including any personal data included in the Customer Data, is described in the DPT and Customer's volume licensing agreement.
- **Customer Data Access**. For the term designated under Customer's volume licensing agreement Microsoft will, at its election and as necessary under applicable law implementing Article 12(b) of the EU Data Protection Directive, either: (1) provide Customer with the ability to correct, delete, or block Customer Data, or (2) make such corrections, deletions, or blockages on Customer's behalf.

Security

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

Online Services Information Security Policy

Each Online Service follows a written data security policy ("Information Security Policy") that complies with the control standards and frameworks shown in the table below.

Online Service	ISO 27002 Code of Practice	ISO 27018 Code of Practice	SSAE 16 SOC 1 Type II	SSAE 16 SOC 2 Type II
Office 365 Services	Yes	Yes	Yes	Yes
Microsoft Dynamics Online Services	Yes	Yes	Yes*	Yes*
Microsoft Azure Core Services	Yes	Yes	Varies**	Varies**

Online Service	ISO 27002 Code of Practice	ISO 27018 Code of Practice	SSAE 16 SOC 1 Type II	SSAE 16 SOC 2 Type II
Microsoft Intune Online Services	Yes	Yes	Yes	Yes
Microsoft Power BI Services	Yes	Yes	No	No

Microsoft Audits of Online Services

For each Online Service, Microsoft will conduct audits of the security of the computers, computing environment and physical data centers that it uses in processing Customer Data (including 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 for each Online Service.
- 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 will be Microsoft's Confidential Information. The Microsoft Audit Report 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 so that Customer can verify Microsoft's compliance with the security obligations under the DPT. The Microsoft Audit Report will be subject to non-disclosure and distribution limitations of Microsoft and the auditor.

If the Standard Contractual Clauses apply, then (1) Customer agrees to exercise its audit right by instructing Microsoft to execute the audit as described in this section of the DPT, and (2) if Customer desires to change this instruction, then Customer has the right to do so as set forth in the Standard Contractual Clauses, which shall be requested in writing.

If the Standard Contractual Clauses apply, then nothing in this section of the DPT varies or modifies the Standard Contractual Clauses or affects any supervisory authority's or data subject's rights under the Standard Contractual Clauses. Microsoft Corporation is an intended third-party beneficiary of this section.