Amendment ID CTM
CTM Amendment 2

**Preamble**

Customer and Microsoft entered into a Microsoft Business and Services Agreement (**MBSA**) as amended, with an effective date of 1 February 2019, with reference Framework-VNG (**CTM Amendment 1**), which was based on a central framework agreement with the Dutch central government. Pursuant to additional arrangements agreed with the Dutch central government and as Microsoft has made several changes to its Online Service Terms (**OST**), Microsoft and Customer agree to add additional items as set out in this amendment (**CTM Amendment 2**).

**Amendment**

The MBSA, CTM Amendment 1, the Enterprise Agreement and the OST of November 2019 and possible future OSTs (collectively defined as **Agreement**) are hereby amended as follows.

If Microsoft changes Product Terms or Use Rights for Online Services that are subscribed to by Affiliates on the effective date of CTM Amendment 2, any provision in such changed Product Terms or Use Rights that conflicts with CTM Amendment 2 shall not apply.

In the event of any conflict between the terms of CTM Amendment 2 and the terms of the MBSA, Enterprise Agreement, any enrollment, any Product Terms, the OST, any orders submitted under any of these terms or agreements, any other documents in these terms or agreements and any other applicable terms or agreements between Microsoft and the Customer and any Affiliate, the terms of CTM Amendment 2 will prevail.

Microsoft and Customer (and any of its Affiliates) cannot deviate from the terms of CTM Amendment 2 unless this is explicitly agreed in a further amendment that explicitly refers to the deviation of the relevant terms of CTM Amendment 2.

The effective date of this CTM Amendment 2 is 1-May-2020.

This CTM Amendment 2 will apply by default to new Enrollments or Enrollments that are renewed and to which this MBSA is applied after the effective date of CTM Amendment 2. For existing Enrollments to which this MBSA applies prior to the effective date of CTM Amendment 2, Enrolled Affiliates can choose to have this CTM Amendment 2 apply during the term of their Enrollment by signing a separate amendment. For existing Enrollments to which this MBSA does not yet apply at the effective date of CTM Amendment 2 or thereafter, Enrolled Affiliates can choose to have the MBSA, as amended through CTM Amendment 1 and CTM Amendment 2, apply by signing a separate remaster amendment.

**Appendix 1: Data Processing Instructions and Limitations**

1. **Definitions**

Capitalized terms used but not defined in this CTM Amendment 2 will have the same meanings as set forth in the Agreement. Lower case terms used but not defined in this CTM Amendment 2, such as “personal data breach”, “processing”, “controller”, “processor”, “profiling”, “personal data”, and “data subject” will have the same meaning as set forth in Article 4 of the GDPR.

The section entitled “Definitions” of the OST is amended by addition of the following, which will be added at the end of the section:

*“Customer User” means a user of an Online Service that is an employee, civil servant, onsite contractor, or onsite agent to whom Customer or one of its Affiliates have assigned a license to use an Online Service.*

*“Diagnostic Data” are data, including telemetry data, collected or obtained, by Microsoft from locally installed software.*

*“System Generated Data” are data generated by Microsoft through the operation of an Online Service.*

*Microsoft acknowledges and agrees that Customer Data, Support Data, Diagnostic Data, System Generated Data, functional data and other data may contain Personal Data.*

1. **Processing of Customer Data**

The sentences “Customer Data will be used or otherwise processed only to provide Customer the Online Services including purposes compatible with providing those services. Microsoft will not use or otherwise process Customer Data or derive information from it for any advertising or similar commercial purposes. Microsoft acquires no rights in Customer Data, other than the rights Customer grants to Microsoft to provide the Online Services to Customer.” in the paragraph entitled “Processing of Customer Data; Ownership” in the “Data Protection Terms” section of the OST, are hereby replaced in their entirety with the following:

***Authorized purposes***

*Customer hereby instructs Microsoft to process Customer Data (including Personal Data therein), including, for the avoidance of doubt any Personal Data that are provided to Microsoft by, or on behalf of Customer or any of the Customer Users or other data subjects through use of an Online Service, together with Personal Data collected or generated by Microsoft in connection with the use by the Customer or any of the Customer Users of an Online Service only where proportional for the following authorized purposes:*

1. *Performing (providing and improving the Online Services, identifying and mitigating anomalies, “bugs,” and other Online Services issues through updates to the Online Services)*
2. *Without prejudice to (a) above, Security (identifying and mitigating security threats and risks)*
3. *Without prejudice to (a) above, Up to date (delivering and installing the latest updates to the Online Services)*

***Microsoft responsibilities***

*With respect to Customer Data (including Personal Data therein), including, for the avoidance of doubt any Personal Data that are provided to Microsoft by, or on behalf of Customer or any of the Customer Users or other data subjects through use of an Online Service, together with Personal Data collected or generated by Microsoft in connection with the use by the Customer or any of the Customer Users of an Online Service, Microsoft shall not process such data in the Online Services that are offered by Microsoft as a data processor for the purpose of:*

1. *data analytics,*
2. *profiling (including but not limited to creating psychometric, psychographic, or other user profiles),*
3. *advertising (including targeted on-screen recommendations for products or services offered by Microsoft but not subscribed to or not used by Customer) or similar commercial purpose, or*
4. *market research aimed at creating new functionalities, services or products or any other purpose;*

*unless this is authorized in accordance with Customer’s documented instructions.*

*The above shall not prevent Microsoft from running its legitimate business operations, to the extent that this does not go beyond:*

1. *billing and preparing invoices,*
2. *account management,*
3. *compensation,*
4. *financial reporting in accordance with legal and stock exchange obligations,*
5. *revenue metrics, pricing, assessing usage of the Online Services, business planning including structuring its business and branding, product strategy, internal executive reports, and capacity modeling and forecasting,*
6. *improving the core functionality of accessibility, privacy, or energy-efficiency,*
7. *combatting fraud, cybercrime and cyber-attacks that may affect any Microsoft product or service, not including discretionary scanning of contents of Customer Data or targeting of Customer Users without prior notice to Customer, or*
8. *complying with Microsoft’s legal obligations, subject to the “Disclosure of Customer Data” provision in the Data Protection Terms of the OST and the confidentiality obligations set forth in the MBSA.*

*provided that Microsoft shall* *not process Customer Data (including Personal Data therein), including, for the avoidance of doubt any Personal Data that are provided to Microsoft by, or on behalf of Customer or any of the Customer Users or other data subjects through use of an Online Service, together with Personal Data collected or generated by Microsoft in connection with the use by the Customer or any of the Customer Users of an Online Service for the purpose of:*

1. *profiling (including but not limited to creating psychometric, psychographic, or other user profiles); or*
2. *advertising (including targeted on-screen recommendations for products or services offered by Microsoft but not subscribed to or not used by Customer) or similar commercial purpose.*

*For the avoidance of doubt, any data disclosed, pseudonymised or de-identified but not anonymized as part of Microsoft’s legitimate business operations, or Personal Data derived from Personal Data as part of Microsoft’s legitimate business operations, may not be used or further used for any other purpose.*

*Microsoft shall ensure that when it anonymizes Personal Data it shall:*

1. *comply with applicable data protection laws and regulatory guidance on anonymisation, in particular with WP29 Opinion 05/2014 on Anonymisation techniques (WP216); and*
2. *ensure that any resulting anonymized data no longer allows for the direct or indirect identification or re-identification of a data subject.*

*When processing resulting anonymized data Microsoft:*

1. *is prohibited from re-identifying any data subjects;*
2. *is prohibited from using the resulting anonymized data to take any measure or decision with regard to specific data subjects; and*
3. *shall notify Customer without undue delay in case it is detected that data subjects can be or have been re-identified.*

*Microsoft shall perform an assessment of the risks regarding the re-identification of data subjects.* *A single assessment may address a set of similar processing operations that present similar risks.*

*To the extent that Microsoft collects or generates data that is neither* *Customer Data (including Personal Data therein) nor Personal Data but that remains identifiable to Customer, Microsoft’s use of such data remains subject to the “Disclosure of Customer Data” provision in the Data Protection Terms of the OST and the confidentiality obligations set forth in the Agreement.*

*For the purposes of this Section and the avoidance of doubt to “process” data includes: to disclose, pseudonymise, de-identify, or anonymise such data, or to process or further process such data in any other manner, to combine such data with other data, or to derive any data or information from such data.*

1. **Documented instructions**

The following replaces the sentence “Microsoft will process Personal Data only on documented instructions from Customer” in the subparagraph “Processor and Controller Roles and Responsibility”) of the paragraph “Processing of Personal Data; GDPR” of the section of the OST entitled “Data Protection Terms”:

“*Unless Microsoft is a controller, Microsoft will process Customer Data and Personal Data only on documented instructions from Customer*.”

1. **Applicable Online Services Terms and Updates**

The paragraph entitled “Applicable Online Services Terms and Updates” in the section “Introduction” of the OST is replaced in its entirety with the following:

**“*Applicable Online Services Terms and Updates***

*When Customer renews or purchases a new subscription to an Online Service, the then-current Online Services Terms will apply and will not change during Customer’s subscription for that Online Service. When Microsoft introduces features, supplements or related software that are new (i.e., that were not previously included with the subscription), Microsoft may provide terms or make updates to the Online Services Terms that apply to Customer’s use of those new features, supplements or related software. The provisions of these Online Services Terms supersede any conflicting provisions of the Microsoft Privacy Statement that otherwise may apply to processing of Customer Data, Personal Data, or Support Data as defined herein.”*

1. **Customer Responsibilities**

The subparagraph entitled “Customer Responsibilities” in the paragraph “Data Security” in the section “Data Protection Terms” of the OST is replaced in its entirety with the following:

***“Customer Responsibilities***

*Customer is solely responsible for making an independent determination as to whether the technical and organizational measures for an Online Service meet Customer’s requirements, including any of its security obligations under the GDPR or other applicable data protection laws and regulations. Microsoft is responsible for implementing, maintaining and following appropriate technical and organizational measures intended to protect Customer Data against accidental, unauthorized or unlawful access, disclosure, alteration, loss, or destruction. Customer is responsible for implementing and maintaining privacy protections and security measures for components that Customer provides or controls (such as devices enrolled with Microsoft Intune or within a Microsoft Azure customer’s virtual machine or application).”*

1. **Installation and Use Rights**

The subparagraph entitled “Installation and Use Rights” as part of the paragraph “Office 365 Applications” in the section “Online Service Specific Terms” of the OST is replaced in its entirety with the following:

*“****Installation and Use Rights***

*Each user to whom Customer assigns a User SL must have a work or school account in order to use the software provided with the subscription. These users:*

* *may activate the software provided with the SL on up to five concurrent OSEs for local or remote use;*
* *may also install and use the software, with shared computer activation, on a shared device, a Network Server, or on shared servers on Microsoft Azure or with a Qualified Multitenant Hosting Partner. A list of Qualified Multitenant Hosting Partners and additional deployment requirements are available at* [*www.office.com/sca*](http://www.office.com/sca)*. This shared computer activation provision does not apply to Customers licensed for Office 365 Business; and*
* *must connect each device upon which user has installed the software to the Internet at least once every 30 days or the functionality of the software may be affected.*
* *may use Internet-connected Online Services provided as part of ProPlus. Additionally, if permitted by Customer, users may elect to use connected services subject to terms of use other than this OST and with respect to which Microsoft is a data controller (such connected services the “Controller Connected Services”), as identified in product documentation.*

*Customer shall have the possibility and be responsible for enabling or disabling the Controller Connected Services.*

*At the effective date of this CTM Amendment 2, Microsoft is a sole controller only for the following Controller Connected Services:*

|  |  |
| --- | --- |
| *3D Maps* | *Help > Contact Support* |
| *Map Charts* | *Help > Suggest a Feature* |
| *Insert Online Pictures* | *Insert online video* |
| *Insert Online 3D Models* | *Microsoft Error Reporting Program (MERP)* |
| *PowerPoint QuickStarter* | *Office Store* |
| *Researcher* | *Research* |
| *Smart Lookup* | *Weather Bar in Outlook* |
| *Resume Assistant* |  |

*Controller Connected Services: Authoritative documentation for Microsoft is now published here: https://docs.microsoft.com/en-us/deployoffice/privacy/optional-connected-experiences*

*This documentation will be changed at any time the status of the available experiences changes.”*

1. **Standard Contractual Clauses – Definitions**

The definition of “Standard Contractual Clauses” in the section “Definitions” of the OST is replaced in its entirety with the following:

*“Standard Contractual Clauses” means the standard data protection clauses for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection, as described in Article 46 of the GDPR and approved by the European Commission decision 2010/87/EC, dated 5 February 2010. The Standard Contractual Clauses are in Attachment 3.”*

1. **Standard Contractual Clauses**

The first paragraph of the section entitled “Introduction” in the OST, is amended by the addition of the following:

*“With respect to Customer Data, in the event of any conflict between the terms of the Standard Contractual Clauses and the terms of the Agreement, any Enrollment, any Product Terms, the OST, any orders submitted under any of these terms or agreements, any other documents in these terms or agreements and any other applicable terms or agreements between Microsoft and the Customer, the terms of the Standard Contractual Clauses will prevail.”*

1. **Subprocessors**

The sentences in the paragraph “Notice and Controls on use of Subprocessors” in the section “Data Protection Terms” of the OST

“From time to time, Microsoft may engage new Subprocessors. Microsoft will give Customer notice (by updating the website and provide Customer with a mechanism to obtain notice of that update) of any new Subprocessor at least 14-days in advance of providing that Subprocessor with access to Customer Data or Personal Data. However, with respect to Core Online Services, Microsoft will give Customer notice (by updating the website and provide Customer with a mechanism to obtain notice of that update) of any new Subprocessor at least 6-months in advance of providing that Subprocessor with access to Customer Data.”

are replaced in their entirety with the following:

*“From time to time, Microsoft may engage new Subprocessors. Microsoft will give Customer notice (by updating the website and provide Customer with a mechanism to obtain notice of that update) of any new Subprocessor at least 14 days in advance of providing that Subprocessor with the ability to process to Customer Data or Personal Data. However, with respect to Core Online Services, Microsoft will give Customer notice (by updating the website and provide Customer with a mechanism to obtain notice of that update) of any new Subprocessor at least 6 months in advance of providing that Subprocessor with access to Customer Data.”*

1. **Suspension**

The following is added to *subsection 5(c) of the Enterprise Agreement*:

“*This subsection 5(c) also applies if Microsoft intends to suspend any Online Service for breach.”*

1. **Acceptable Use Policy**

Microsoft confirms that the sentence “Violation of the terms in this section may result in suspension of the Online Service.” only applies to the wording under the header “Acceptable Use Policy”.

1. **Data retention**

The following wording will be added to the paragraph “Data Retention and Deletion” of the section entitled “Data Protection Terms”

*“At the date of the execution of CTM Amendment 2, the maximum retention period for diagnostic data in Office 365 ProPlus is 18 months from the date the data is received by Microsoft.”*

1. **Consent**

Section 4(a) of the Agreement is hereby replaced in its entirety with the following:

“**(a)** *Each party is obliged to ensure that the provision of personal information or other data to the other party complies with the privacy laws, data protection laws and other legal provisions (e.g., contractual) applicable to the respective party, before providing such data to the other party*. *This includes Customer’s consent to the processing of personal information by Microsoft and its agents to facilitate the subject matter of this agreement for jurisdictions where such consent is legally available and required.”*

1. **Applicability to other Products and Professional Services**

Microsoft acknowledges that Customer may require that the principles contained in this CTM Amendment 2, wherever relevant, also be applied to other Products and Professional Services in order for Customer to either continue or initiate usage of such products and services. Accordingly, subject to further analysis and discussions, Microsoft agrees to undertake a review to extend these principles to additional Products and Professional Services.

1. **Security Incident Notification**

Item 23 as included in CTM Amendment 1 (related to OST paragraph entitled “Security Incident Notification”) is deleted in its entirety.

**Appendix 2: Centralized Audit Framework**

1. **Auditing Compliance**

Item 9 as included in CTM Amendment 1 (adding a new subsection entitled “Audit and Right to Instruct” to section 4 “Privacy and Compliance with Laws” of the MBSA) is hereby deleted. The following sentences from the OST are hereby deleted:

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

The following sentences from the OST are hereby deleted:

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

The subparagraph entitled “Auditing Compliance” in the paragraph “Data Security” in the section “Data Protection Terms” of the OST is amended by the addition of the following:

**“Customer Data and Personal Data Audit Rights for Customer**

Should Customer wish to exercise its audit rights under the Standard Contractual Clauses or the GDPR, Microsoft shall make the processing systems, facilities and supporting documentation relevant to the processing of Customer Data and Personal Data by Microsoft, its Affiliates, and its Subprocessors available for audit by Customer, all to the extent that inspection of the foregoing is relevant for the purpose of the audit of the data processing. For these audit purposes, Customer hereby designates the single representative appointed by the Dutch Ministry of Justice (the MoJ Representative) and agrees to participate in the audit conducted under a central framework managed through this representative (the Dutch Centralized Audit Framework). The audit will always be performed by a qualified independent third-party auditor selected and funded by such representative of Customer. Such independent third-party auditor will sign a market standard non-disclosure agreement with Microsoft.

The purpose of the audit shall be to confirm Microsoft’s compliance with its obligations with respect to the processing of Customer Data and Personal Data under the Standard Contractual Clauses, GDPR and this OST, as amended, for the Online Services Customer or its Affiliates are using.

Microsoft shall provide, and must ensure that the relevant Subprocessors provide, all reasonable assistance and explanations to the auditors, in an open and transparent manner, subject to mutual agreement on scope, process, and cost thereof as agreed with the MoJ Representative. Pursuant to such agreement, Customer will use best efforts to prevent or minimise any disruption to the operations of Microsoft, and Customer will ensure that persons conducting an audit comply with Microsoft’s applicable process, safety and security requirements while conducting the audit. The auditors shall not have access to any data from Microsoft’s other customers or to Microsoft systems or facilities not involved in the Online Services.

Due to the shared service nature of Online Services, and the practical constraints associated with audit activity, and without prejudice to the Standard Contractual Clauses and the GDPR audit rights of Customer acting as data controller, Customer and Microsoft will first attempt other possible measures to satisfy a data processing verification requirement but such attempts may not be used by Microsoft to delay an audit. An audit may be carried out as many times as Customer requires through the Dutch Centralized Audit Framework. Unless otherwise requested by Customer or the MoJ Representative, within 5 business days of written request from the MoJ Representative to commission an audit, Microsoft shall commence, perform and agree with no undue delay, preparation for a Customer audit by the MoJ Representative. Preparation comprises mutual agreement of:

1. The Online Services that Customer is using that are to be in scope of the audit;
2. The data processing outcomes, information, and control requirements to be in scope of the audit evidence requirements;
3. The nature and process for satisfactory audit evidence (for example: view of Microsoft internal documentation or systems, inspection of Microsoft facilities, consultation with Microsoft subject matter experts);
4. The location, and scheduling for the audit activities necessary to accomplish the above, provided that this requirement to agree scheduling shall not permit Microsoft to unreasonably delay performance of the audit; and
5. Inventory of the Microsoft resources needed to conduct the above and calculation of the fees for audit.

|  |  |
| --- | --- |
| Audit Resource | Microsoft Fees |
| Microsoft Online Services Engineering Design or Operations staff, Regulatory Compliance program managers, Operational Security Professionals and similar SME’s working in the performance of Online Services | The **lesser** rate of:1. US $4000 per day of work; or
2. The highest daily rate for Microsoft consulting resources on a Professional Services rate card in effect between Microsoft and the Dutch Ministry of Justice at the time of the audit preparation.

Either of the above shall include applying the fee basis to (reasonable, pre-agreed during audit preparation) preparation time pertaining to customer-specific evidence requirements and the performance of audit evidence presentations or explanations.Fees will be prorated hourly for less than a full 8 hour day of work.All fees will be agreed in advance for the audit objectives finalized during audit preparation.Mutually agreed Professional Service change management will be used to agree in advance additional or changed audit objectives and concomitant additional or changed fees arising. |
| Travel expenses of Microsoft personnel involved in audit | In accordance with Microsoft’s then current published Professional Services travel expenses policy, to be provided in advance during audit preparation. |
| Account aligned Microsoft resources | No fees |
| Admin staff, document preparation and similar logistical matters | No fees  |
| Use of any Microsoft facility | No fees for use during an audit activity. |

After completion of the audit preparation, the audit will be conducted as prepared.

Microsoft and Customer bear their own costs and expenses of any audit, provided that the Microsoft audit fees shall be payable by the MoJ Representative on behalf of the Customer and any other Dutch public sector customers that are part of the central framework managed through this representative under the terms of the Dutch Ministry of Justice’s agreement with Microsoft. If the audit report generated as a result of Customer’s audit includes any finding of material non-compliance, Customer shall share such audit report with Microsoft and Microsoft shall promptly cure any material non-compliance.

No Microsoft audit fee shall be payable by the MoJ or the Customer if:

* Customer undertakes an audit of Microsoft as a result of an investigation by Customer’s supervisory authority for GDPR compliance to which Customer is obligated to respond and where the investigation requires Customer’s audit of Microsoft as Customer’s processor or Subprocessor; or
* After a Security Incident, Customer wishes to audit the technical and organizational measures implemented by Microsoft to remediate the root cause of such Security Incident.

If an audit results in the parties becoming aware of a Security Incident not previously addressed by Microsoft as set forth in the section of the OST entitled “Security Incident Notification,” Microsoft will promptly and at its cost take all remedial actions identified therein, including where relevant retrieving from third parties all Customer Data, Personal Data and other data that were disclosed by Microsoft in breach of this Amendment and prohibit further use thereof by such third parties.

Subject to the above, Customer shall through the MoJ Representative:

1. give Microsoft reasonable notice of the intention to perform an audit pursuant to this section and participate fully in the audit scoping efforts;
2. procure that the qualified independent assessor performing the audit comply with Microsoft’s reasonable confidentiality and health and safety regulations, as notified by Microsoft to Customer; and
3. procure that its representatives and nominees conducting the audit use reasonable efforts to minimise any disruption to Microsoft's business caused by the performance of the audit.

All of Customer's rights and Microsoft’s obligations as set out in this section shall remain in force until six months after the termination or expiration of the relevant agreements between Microsoft and Customer have passed.

This OST Amendment does not in any way limit the Customer’s rights to information, audits and inspections under the Standard Contractual Clauses and the GDPR.”

**Appendix 3: Check-Box Instructions**

1. **Processing of Personal Data; GDPR**

The subparagraph entitled “Processing Details” in the paragraph entitled “Processing of Personal Data; GDPR” in the “Data Protection Terms” section of the OST is replaced in its entirety with the following:

***“Processing Details***

*The parties acknowledge and agree that:*

* *The subject-matter of the processing is limited to Personal Data within the scope of the “Processing of Customer Data; Ownership” in the “Data Protection Terms” section of the OST and the GDPR;*
* *The duration of the processing shall be for the duration of the Customer’s right to use the Online Service and until all Personal Data is deleted or returned in accordance with Customer instructions or the terms of the OST;*
* *The nature and purpose of the processing shall be to provide the Online Service pursuant to Customer’s volume licensing agreement, inclusive of the section of this OST entitled “Processing of Customer Data; Ownership,” above;*
* *The types of Personal Data processed by the Online Service include Customer Data including the categories of Personal Data set forth in Appendix 1 to Attachment 3 – The Standard Contractual Clauses (Processors) of the OST and other Personal Data including Diagnostic Data, System Generated Data and functional data, including as described in the service trust portal (https://aka.ms/stp) and applicable Online Services documentation (https://docs.microsoft.com); and*
* *The categories of data subjects are Customer’s representatives and end users, such as employees, contractors, collaborators, and customers and the data subjects listed in Appendix 1 to Attachment 3 – The Standard Contractual Clauses (Processors) of the OST.”*
1. **Model Clauses to convey the categories of personal data**

The Microsoft entity signing this CTM Amendment 2 will cause Microsoft Corporation to replace the paragraphs “Data subjects” and “Categories of data” in Annex 1 to Attachment 3 – The Standard Contractual Clauses (Processors) of the OST in their entirety with Annex 1 as attached hereto. For the avoidance of doubt, individual Affiliates are not required to provide their input to Microsoft with regards to Annex 1 to Attachment 3, but if required can maintain a completed version of Annex 1 to Attachment 3 in their administration.

**Annex 1 to Appendix 3**

**The Standard Contractual Clauses (Processors)**

 **Categories of Data Subjects**

The personal data transferred concern the following categories of data subjects (please specify):

□ Employees, contractors and temporary workers (current, former, prospective) of data exporter (governmental organization);

□ Dependents of the above;

□ Data exporter's collaborators/contact persons (natural persons) or employees, contractors or temporary workers of legal entity collaborators/contact persons (current, prospective, former);

□ Citizen users (customers, clients, patients, visitors, etc.) and other data subjects that are users of data exporter's governmental services;

□ Citizens, partners, stakeholders or individuals who actively collaborate, communicate or otherwise interact with employees of the data exporter and/or use communication tools such as apps and websites provided by the data exporter;

□ Citizens, stakeholders or individuals who passively interact with data exporter, because they are the subject of an investigation, research or mentioned in documents or correspondence from or to the data exporter;

□ Minors;

□ Professionals with professional privilege (doctors, lawyers, notaries, religious workers, etcetera);

□ Others, this should be noted here: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

**Categories of Data**

The personal data transferred concern the following categories of data (please specify):

□ Basic personal data – such as place of birth, street name and house number (address), postal code, city of residence, country of residence, mobile phone number, first name, last name, initials, email address, gender, date of birth

□ basic personal data about family members and children;

□ authentication data user name, password or PIN code, security question, audit trail;

□ Contact information - such as addresses, email, phone numbers, social media identifiers; emergency contact details;

□ Unique identification numbers and signatures - such as Taxpayer ID (VAT number), National ID (BSN), social security number, bank account number, passport and ID card number, driver's license number and vehicle registration data, IP addresses, license plate number, employee number, student number, patient number, signature, unique identifier in tracking cookies or similar technology such as browser fingerprint;

□ Pseudonymous Identifiers;

□ Financial and insurance information (for example insurance number, bank account name and number, creditcard name and number, invoice number, income, type of assurance, payment behaviour, creditworthiness);

□ Commercial Information; for example history of purchases, special offers, subscription information, payment history;

□ Biometric Information, such as DNA, fingerprints and iris scans;

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

□ Photos, video and audio;

□ Internet activity - browsing history, search history, reading, television viewing, radio listening activities;

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

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

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

□ Education data, such as education history, current education, grades and results, highest degree achieved, learning disability;

□ Citizenship and residency information, for example citizenship, naturalisation status, marital status, nationality, immigration status, passport data, details of residency or work permit;

□ Judicial information and criminal records (not falling under “Special Categories of Data” below);

□ Information processed for the performance of a task carried out in the public interest or in the exercise of an official authority, this should be noted here: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;

□ Other information, this should be noted here: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

**Special Categories of Data (if appropriate)**

The personal data transferred concern the following special categories of data (please specify):

□ None;

□ If you are transferring or using any information about an individual’s racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, data concerning a natural person’s sex life or sexual orientation, data relating to criminal convictions or offences, this should be noted here: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

**Processing operations**

The personal data transferred will be subject to the following basic processing activities (please specify):

The processing activities restricted to the processing of Customer Data for the purposes as specified in section 3 of this CTM Amendment 2.

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



**Appendix 4: Additional Microsoft Countersignature**

1. **Attachment 5 – Data processor agreement**

The Microsoft entity signing this CTM Amendment 2 will cause Microsoft Corporation to add a new Attachment 5, titled “Data processor agreement”, to be added to the OST with the following wording:

“*Microsoft Corporation agrees to the “Data Protection Terms” in the OST as a data processor agreement with Customer. References in the “Data Protection Terms” to “Microsoft” notifying Customer may be satisfied by a notification either by Microsoft Corporation or Microsoft Ireland Operations Limited.”*

