


Data Transfer Impact Assessment (DTIA) on the transfer of Content Data to the USA via Teams		 <small>This DTIA was made by Privacy Company and SLM Rijk, using and adapting the template provided by David Rosenthal, provided under CC license</small>		
<b>Step 1: Describe the intended transfer</b>				
a)	Data exporter (or the sender in case of a relevant onward transfer):	[University X/ Dutch government organisation Y]		
b)	Country of data exporter:	Netherlands		
c)	Data importer (or the recipient in case of a relevant onward transfer):	Microsoft Corp. USA		
d)	Country of data importer:	USA, Microsoft also has data centers in the EU		
e)	Context and purpose of the transfer:	Employees of the MOJ or any other Governmental entity using Teams for work purposes		
f)	Categories of data subjects concerned:	Employees of the Dutch government, and possibly external data subjects which have a working relationship with MOJ or any other governmental organisation and therefore could participate in the online communications.		
g)	Categories of personal data transferred:	contents of communication, including text, sound, video, and image files exchanged for work purposes. See the separate DTIAs for Account Data, Diagnostic Data (Telemetry and Service Generated Server Logs), Support Data, and cloud Storage of recordings and transcriptions		
h)	Sensitive personal data:	Teams Conversations may include sensitive data (for example location data, salary information, company or personal confidential information), data relating to children under 16 years, special categories of data and data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation (Art. 9 GDPR). Conversations may also include personal data relating to criminal convictions and offences or related security measures (Art. 10 GDPR).		
i)	Technical implementation of the transfer:	The streaming content from EU Enterprise and Education customers is processed on Microsoft servers in the EU. Nonetheless, personal data included in the streaming content can be accessed by Microsoft employees in the USA since the Teams conversations are facilitated by servers controlled and managed by Microsoft Corp.		
j)	Technical and organizational measures in place:	Microsoft does not yet offer end-to-end encryption (e2ee) for the streaming communication with multiple participants in Teams, only for unscheduled one-to-one video calls. The streaming data can be accessed by Microsoft in the USA. Microsoft can be compelled to disclose personal data to security services and law enforcement authorities in the USA, in spite of its encryption measures. Media traffic in Teams is encrypted with Secure RTP (SRTP). Data processed in data centres are encrypted with 256-bit AES encryption. The applied encryption is FIPS 140-2 compliant. Keys are stored in the Azure Key Vault.		
k)	Relevant onward transfer(s) of personal data (if any):	For streaming content, there is no onward transfer. Streaming data is part of Customer Content. Microsoft currently per the DPA ( <a href="https://aka.ms/dpa">https://aka.ms/dpa</a> ) provides data residency commitments on customer content at rest. Subprocessors by policy do not have access to customer content for the services in scope. Microsoft will not unilaterally store any audio or video content from such Audio/Video calls or meetings, therefore when assuming a risk that the US government could compel Microsoft to turn over data stored in the EU from such calls, the audio and video would not be available in such a scenario. Only if a user initiates a recording would there be stored audio or video content of a call		
l)	Countries of recipients of relevant onward transfer(s):	Microsoft provides data residency commitments for Microsoft Office 365 for Customer Data at rest, and document additional commitments for Teams and compute here: <a href="https://docs.microsoft.com/en-us/microsoft-365/enterprise/eu-data-storage-locations?view=o365-worldwide">https://docs.microsoft.com/en-us/microsoft-365/enterprise/eu-data-storage-locations?view=o365-worldwide</a> .		
<b>Step 2: Define the DTIA parameters</b>				
<b>Rationale</b>				
a)	Starting date of the transfer:	[fill in date]		
b)	Assessment period in years:	2		
c)	Ending date of the assessment based on the above:	X+2		
d)	Target jurisdiction for which the DTIA is made:	USA		
e)	Is importer an Electronic Communications Service Provider as defined in USC § 1881(b)(4):	Yes		
f)	Does importer/processor commit to legally resist every request for access:	Yes		
g)	Relevant local laws taken into consideration:	Section 702 FISA, other FISA warrants such as business records, pen registers and trap and trace devices, EOP 12333 (mitigated by PPD-28), National Security Letters (secret services) and US Cloud Act, US Stored Communications Act (SCA), NSLs based on ECPA, administrative and judicially issued subpoenas, and search warrants.		
<p><i>This DTIA takes the risks of two types of US legislation into account: traditional law enforcement, and court ordered subpoenas and warrants, as well as secret services powers, letters and FISC authorisations. Since Microsoft is an Electronic Communications Service Provider, EOP 12333 and FISA Section 702 also apply directly to Microsoft, and not only to backbone providers addressed in Step 4b of this DTIA. Microsoft also qualifies as "remote computing services" or "electronic communication services". This means the US Stored Communications Act and US CLOUD Act also apply. This DTIA does "not" assess the risks of requests for personal data ordered by EU law enforcement authorities through MLAT requests. This DTIA also cannot take the risks into account of the recently disclosed CIA bulk surveillance based on EOP 12333, as it is not known what categories of personal data this surveillance involves.</i></p>				
<b>Step 3: Probability that a foreign authority has a legal claim in the data and wishes to enforce it against the provider</b>				
		Probability per case	Cases per year	Cases remaining
<b>Rationale</b>				
a)	Number of cases under the laws listed in Step 2g per year in which an authority in the USA is estimated to attempt to obtain relevant data through legal action during the period under consideration.		0,50	
<p><i>The number of 0.5 case per year is an estimate based on (1) Microsoft's own transparency reporting and assurance it has not yet provided any personal data from EU public sector customers to any government*, (2) historical data available in this sector, and (3) a requirement to calculate based on a number greater than zero. *For clarity, under US law, providers can neither confirm nor deny having received any specific legal demands subject to a secrecy obligation.</i></p>				
b)	Share of such cases in which the request occurs in connection with a case that due to its nature in principle permits the authority to obtain the data also from a provider	100%	0,50	
<p><i>Some streaming Content Data, such as chats, are by its nature accessible in the clear. Other Teams Content Data can be made accessible by Microsoft, as E2EE is currently only available for unscheduled 1-on-1 conversations. Microsoft promises to legally resist every order, pay compensation to its customers when it is compelled to disclose, and Microsoft is a processor, not a data controller for the Content Data.</i></p>				
c)	Probability that in the remaining such cases it will be possible for the company to successfully cause the authority (by legal means or otherwise) to give up its request for the data in plain text	10%	0,45	
<p><i>Some streaming Content Data, such as chats, are by its nature accessible in the clear. Other Teams Content Data can be made accessible by Microsoft, as E2EE is currently only available for unscheduled 1-on-1 conversations. Microsoft promises to legally resist every order, pay compensation to its customers when it is compelled to disclose, and Microsoft is a processor, not a data controller for the Content Data.</i></p>				
d)	Probability that in the remaining cases the requested data will be provided in one way or another (e.g., with consent or through legal or administrative assistance)	50%	0,23	
<p><i>Consent from an EU Enterprise or EDU Customer is unlikely, in the absence of an adequate treaty with the USA. Since Microsoft is a processor, and not a controller for the Content Data, it will take time for the US authorities to force Microsoft to provide the requested data. Therefore, the chance that the authorities will want to undergo such trouble is limited to only particularly important cases, thus significantly reducing the number of relevant cases.</i></p>				
e)	Probability that in the remaining cases the authority will consider the data it is seeking to be so important that it will look for another way to obtain it	10%	0,02	0,02
<p><i>It is assumed this question tries to assess the probability that Microsoft is hacked. This cannot be excluded.</i></p>				
Number of cases per year in which the question of lawful access by a foreign authority arises			0,02	
Number of cases in the period under consideration			0,05	
<b>Step 4a: Probability that a foreign authority will successfully enforce the claim through the provider</b>				
Section 702 FISA, other FISA warrants such as business records, pen registers and trap and trace devices, EOP 12333 (mitigated by PPD-28), National Security Letters (secret services) and US Cloud Act, US Stored Communications Act (SCA), NSLs based on ECPA, administrative and judicially issued subpoenas, and search warrants.				
<b>Legal Basis considered for the following assessment:</b>				
<b>Prerequisite for success</b>		<b>Probability per case</b>		<b>Rationale</b>
a)	Probability that the authority is aware of the provider and its subcontractors (prerequisite no. 1)	100%	100%	Microsoft is a well-known communications provider with a substantial amount of Enterprise and Edu Customers in the EU
b)	Probability that an employee of the provider or its subcontractors will gain access to the data in plain text in a support-case ... (prerequisite no. 2)	100%	100,00%	Microsoft can be compelled to lift its own encryption on all Teams conversations and chats, as they cannot be encrypted with E2EE, except for unscheduled 1-on-1 conversations.
	... and is able to search for, find and copy the data requested by the authority (prerequisite no. 3)	100%		Microsoft can be compelled to lift its own encryption on all Teams conversations and chats, as they cannot be encrypted with E2EE, except for unscheduled 1-on-1 conversations.
c)	Probability that despite the technical countermeasures taken, employees of the provider, of its subcontractors or of the parent company technically have access to data in plain text (also) outside a support situation (e.g., using admin privileges) or are able to gain such access, e.g., by covertly installing a backdoor or "hacking" into the system (irrespective of whether they are allowed to do so) ... (prerequisite no. 2)	100%	100,00%	Microsoft can be compelled to lift its own encryption on all Teams conversations and chats, as they cannot be encrypted with E2EE, except for unscheduled 1-on-1 conversations.
	... and are then able to search for, find and copy the data requested by the authority (prerequisite no. 3)	100%		Microsoft can be compelled to lift its own encryption on all Teams conversations and chats, as they cannot be encrypted with E2EE, except for unscheduled 1-on-1 conversations.

d)	Probability that the provider, the subcontractor or its parent company, respectively, is located within the jurisdiction of the authority (prerequisite no. 4)	100%		100%	Microsoft is a US based company and has access to its EU data centres																																					
e)	Probability that despite the technically limited access and the technical and organizational countermeasures in place, the authority is permitted to order the provider, its subcontractor or the parent company, respectively, to obtain access to the data and produce it to the authority in plain text (prerequisite no. 5)	10%		10%	Speculative estimate, Microsoft lacks historical data on such scenarios and cannot provide a fact based rationale. It is technically unlikely that Microsoft would be ordered to intercept an ongoing call, or wiretap future conversations from specific individuals.																																					
f)	Probability that if data were to be handed over to the foreign authority, this would lead to the criminal liability of employees of the provider or its subcontractors, the prosecution of which would be possible and realistic, and as a consequence, the data does not have to be produced or is not produced (prerequisite no. 6)	80%		20%	As data importer Microsoft Corporation implements strict technical and organisational measures to protect access to the streaming data (as processed in the EU). These measures are set forth in Microsoft Security Policy and shall comply with the requirements in ISO 27001, ISO 27002, and ISO 27018. Microsoft employs least privilege access mechanisms to control access to Customer Data and Professional Services Data (including any Personal Data therein). Role-based access controls are employed to ensure that access to Customer Data and Professional Services Data required for service operations is for an appropriate purpose and approved with management oversight. For Core Online Services and Professional Services, Microsoft maintains Access Control mechanisms described in the table entitled "Security Measures" in Appendix A of its DPA. For Core Online Services, there is no standing access by Microsoft personnel to Customer Data and any required access is for a limited time. Microsoft would certainly take action if its employees in the USA, or employees of subprocessors, would attempt to unduly access the streaming data.																																					
g)	Probability that the company does not succeed in removing the relevant data in time or otherwise withdrawing it from the provider's access (prerequisite no. 7)	100%		100%	Microsoft can be compelled to lift its own encryption on all Teams conversations and chats, as they cannot be encrypted with E2EE, except for unscheduled 1-on-1 conversations. In case of such a wiretap, Microsoft is legally prohibited from informing its customer.																																					
Residual risk of successful lawful access by a foreign authority through the provider (given the countermeasures):				2,00%																																						
<b>Step 4b: Probability of foreign lawful access by mass surveillance contents</b>																																										
Legal Basis considered for the following assessment: Section 702 US Foreign Intelligence Surveillance Act (FISA), Executive Order (EO) 12333																																										
			<b>Probability in the period</b>	<b>Rationale</b>																																						
a)	Probability that the data at issue is transmitted to the provider or its subcontractors in a manner that permits the telecommunications providers in the country to view it in plain text as part of an upstream monitoring of internet backbones	0%	0,00%	TLS encryption																																						
b)	Probability that the data transmitted will include content picked by selectors (i.e., intelligence search terms such as specific recipients or senders of electronic communications)	0%	0,00%	TLS encryption																																						
c)	Probability that the provider or a subcontractor in the country is technically able to on an ongoing basis search the data in plain text for selectors (i.e. search terms such as certain recipients or senders of electronic communications) without the customer's permission as part of a downstream monitoring of online communications	0%		TLS encryption																																						
d)	Probability that the provider or a subcontractor in the country above may be legally required to perform such as search (also) with the company's data	5%		It is plausible that some Content Data, including chats, from an EU gov or university organisation are interesting for law enforcement and/or security services. Even if processed on EU servers, the data can be decrypted and accessed by Microsoft in the USA if ordered to do so.																																						
e)	Probability that the data is regarded as content that is the subject of intelligence searches in the country as per the above laws	100%		It is plausible that some Content Data, including chats, from an EU gov or university organisation are interesting for law enforcement and/or security services. Even if processed on EU servers, the data can be decrypted and accessed by Microsoft in the USA if ordered to do so.																																						
Residual risk of successful lawful access by a foreign intelligence service without any guarantee of legal recourse (in view of the countermeasures):				0,00%																																						
<b>Step 5: Overall assessment</b>																																										
Probability that the question of lawful access via the cloud provider will arise at all (1 case in the period = 100%)				4,50%																																						
Probability of successful lawful access by the foreign authorities concerned in these cases despite the countermeasures				2,00%																																						
Probability of additional successful lawful access by a foreign intelligence service where there is no guarantee of legal recourse (despite countermeasures)				0,00%																																						
<b>Overall probability of a successful lawful access to data in plain text via the cloud provider in the observation period:</b>				<b>0,09%</b>																																						
Description in words (based on Hillson*):			Very low																																							
The number of years it takes for a lawful access to occur at least once with a 90 percent probability:			∞																																							
The number of years it takes for a lawful access to occur at least once with a 50 percent probability: – assuming that the probability neither increases nor decreases over time (like tossing a coin)			∞																																							
* Scale: <5% = "Very low", 5-10% = "Low", 11-25 = "Medium", 26-50% = "High" and >50% = "Very high" (by David Hillson, 2005, see https://www.pml.org/learning/library/describing-probability-limitations-natural-language-7556)																																										
<b>Step 6: Data subject risks</b>																																										
a)	Estimated probability of occurrence of successful lawful access risk:	0,09%	Very Low	<b>Rationale</b>																																						
b)	Estimated impact of risk	4= special categories of data in the clear	Very High	The streaming content can include special categories of data. Organisations are advised not to use Teams to exchange these data unless the data are already public (such as court hearings or university lectures), or until Microsoft offers E2EE for all exchanges. If organisations only exchange 'regular' personal data, or only use Teams for unscheduled 1-on-1 calls, and possibly use pseudonyms for employees whose identity should remain confidential, the risk is low.																																						
<table border="1"> <tr> <td>Very High</td> <td>Low</td> <td>High</td> <td>High</td> <td>High</td> <td>High</td> </tr> <tr> <td>High</td> <td>Low</td> <td>Medium</td> <td>High</td> <td>High</td> <td>High</td> </tr> <tr> <td>Medium</td> <td>Low</td> <td>Medium</td> <td>Medium</td> <td>High</td> <td>High</td> </tr> <tr> <td>Low</td> <td>Low</td> <td>Low</td> <td>Medium</td> <td>Medium</td> <td>High</td> </tr> <tr> <td>Very Low</td> <td>Low</td> <td>Low</td> <td>Low</td> <td>Low</td> <td>High</td> </tr> <tr> <td></td> <td></td> <td>0</td> <td>1</td> <td>2</td> <td>3</td> <td>4</td> </tr> </table>			Very High	Low	High	High	High	High	High	Low	Medium	High	High	High	Medium	Low	Medium	Medium	High	High	Low	Low	Low	Medium	Medium	High	Very Low	Low	Low	Low	Low	High			0	1	2	3	4	High		
Very High	Low	High	High	High	High																																					
High	Low	Medium	High	High	High																																					
Medium	Low	Medium	Medium	High	High																																					
Low	Low	Low	Medium	Medium	High																																					
Very Low	Low	Low	Low	Low	High																																					
		0	1	2	3	4																																				
<b>Step 7: Define the safeguards in place</b>																																										
<b>Rationale</b>																																										
a)	Would it be feasible, from a practical, technical and economical point of view, for the data exporter to transfer the personal data in question to a location in a whitelisted country instead?	Yes	Describe why you still do not pursue this option	Microsoft has announced that by the end of 2022 the EU data boundary shall be in place for all EU customers. However, this EU data boundary solution does not seem to prevent access to the servers from the USA, because Microsoft is a US-based company.																																						
b)	Is the personal data transferred under one of the exemptions pursuant to applicable data protection law (e.g., Art. 49 GDPR in case of the GDPR)?	No		Only if end users travel to a third country without adequate data protection, and decide to use their Dutch Teams license for work purposes. In that case, the transfer may be based on Art. 49(1)(b) of the GDPR, the transfer is necessary for the performance of a contract between the data subject and the controller.																																						
c)	Is the personal data at issue transmitted to the target jurisdiction in clear text (i.e. there is no appropriate encryption in-transit)?	No	Ensure that data remains encrypted	Strong recommendation to admins not to share special categories of personal data in Teams conversations. Additionally, all traffic over the internet to Microsoft USA is protected by encryption in transit (SSL/TLS).																																						
d)	Is the personal data at issue accessible in the target jurisdiction in clear text by the data importer/recipient or a third party (i.e. the data is either not appropriately encrypted or access to the keys to decrypt is possible)?	Yes	Foreign lawful access is at least technically possible	Yes																																						
e)	Is the personal data at issue protected by a transfer mechanism approved by the applicable data protection law (e.g., the EU Standard Contractual Clauses in case of the GDPR, approved BCR, or - in the case of an onward transfer - a back-to-back-contract in line with the EU SCC), and can you expect compliance with it, insofar permitted by the target jurisdiction, and judicial enforcement (where applicable)?	Yes	Ensure that the mechanism remains in place and is complied with	SLM Rijk and Microsoft have signed the SCCs which have been in place ever since 2010, and are in the process of updating those to the most recently issued version. Microsoft has updated SCCs in place with all third-party subprocessors in India, China or Serbia mentioned in Microsoft Online Services Subprocessors List.																																						
Based on the answers given above, the transfer is:				Not Permitted	Admins should apply E2EE if they want to use Teams for the exchange of special categories of data, when Microsoft makes this available																																					

<b>Final Step: Conclusion</b>							
<b>In view of the above and the applicable data protection laws, the transfer is:</b>							

This Transfer Impact Assessment has been made by:  
 SLM Rijk / PRIVACY COMPANY

Place, Date:

Signed: \_\_\_\_\_  
 By: [Government org X, University Y]