Data Transfer Impact Assessment (DTIA) on the transfer of Support Data to the USA

Step 1: Describe the intended transfer

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:	Ability to receive Customer Support when using Microsoft Support with issues relating to the Microsoft services.
f)	Categories of data subjects concerned:	employees/workers and students/pupils with professional Education or Enterprise Microsoft accounts of the [University X/government organisation Y]
g)	Categories of personal data transferred:	Account Data, Diagnostic Data and possibly recorded or transcribed contents of communications, including text, sound, video, and image files. See the separate DTIAs for Account Data, Diagnostic Telemetry Data and Stored Content
h)	Sensitive personal data:	Support Data may include sensitive Account Data, if an employee works for a government organisation with a high level of sensitivity. Support Data can include Diagnostic Data that may reveal social graphs and working/study patterns. If a customer provides recorded or transcribed conversations as part of a support ticket, this 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). Recorded or transcribed 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:	Personal data are transferred to Microsoft and subprocessors when filing support tickets, and when Microsoft processes the support requests.
j)	Technical and organizational measures in place:	Admins can pseudonymise Account Data (collected in the service generated server logs) by using SSO. Microsoft has announced (in May 2021) that after completion of its "EU Data Boundary" as planned by the end of 2022, Support requests from EU customers will be processed in the EU. Microsoft currently still employs subprocessors for Support Data in third countries. Microsoft explains in the subprocessor list: "*The following subprocessors provide contract staff that work in close coordination with Microsoft employees to help support, operate, and maintain the Microsoft Online Services and in the course of doing so may be exposed to customer data or personal data. In all such cases, customer data or personal data resides only in Microsoft facilities, on Microsoft systems, and subject to Microsoft policies and supervision. For example, a subprocessor may perform remote troubleshooting on a Microsoft server and in the course of doing so may be exposed to snippets of customer data in a server crash dump log.*"
k)	Relevant onward transfer(s) of personal data (if any):	Yes, but only incidentally to Microsoft support employees in the third countries China, Serbia and India. Microsoft has explained it has a worldwide network of support subprocessors, separate and distinct from the Microsoft Online Services subprocessors, to deliver support maximizing for time zone availability, product specific technical and language proficiency, and cost / efficiency. Microsoft has a "follow-the-sun" support model to ensure critical cases have 24/7 coverage until resolution. Customers are in sole control of what data they provide to Microsoft in the context of a support interaction. The only personal data provided to Microsoft in connection with support are the data actively shared in a support ticket by a customer. In the rare case that access to Online Services - and specifically to any personal data in customer's Online Services is necessary to remediate a support issue, the customer may request to be apprised of the escalation process. In the case of services supporting Customer Lockbox (e.g., Exchange Online or SharePoint Online), the customer is advised to configure Lockbox to be able to approve such access for any services operations. All subprocessors in the "contract staff" category perform labor force augmentation services where the personal data remains only in Microsoft facilities on Microsoft systems and subject to Microsoft policies and supervision. The use of subprocessors in this manner does not expose customers to any appreciable incremental risk of government requests for their data, because between the subprocessors and Microsoft, the data remains continuously in Microsoft possession, custody, and control (including without limitation subject to all technical and organizational measures defined and implemented by Microsoft). Even though such access may qualify as an onward transfer, no separate DTIAs have been performed, since this access will stop by the end of 2022, when Microsoft completes its EU Data Boundary.
l)	Countries of recipients of relevant onward transfer(s):	Organisations are strongly advised not to share any non-pseudonymised and special categories of personal data in support tickets prior to the completion of the EU Data Boundary by the end of 2022.

Step 2: Define the DTIA parameters

			Rationale
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.	*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 als 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.*

Step 3: Probability that a foreign authority has a legal claim in the data and wishes to enforce it against the provider

		Probability per case	Cases per year	Cases remaining	Rationale
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		*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.*
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		*Support tickets are encrypted by Microsoft during transport, but are accessible for Microsoft employees in the clear, in controlled and secure environments. 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 personal data.*
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**	100%	0,00		*Support tickets are encrypted by Microsoft during transport, but are accessible for Microsoft employees in the clear, in controlled and secure environments. 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 personal data.*
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)	25%	0,00		*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 personal data in these logs, it will take time for the US authorities to force Microsoft to provide the requested data. Because support requests reveal limited information, 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.*
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%	0,00	0,00	*It is assumed this question tries to assess the probability that Microsoft or its subprocesors are hacked. This cannot be excluded.*
	Number of cases per year in which the question of lawful access by a foreign authority arises			0,00	
	Number of cases in the period under consideration			0,00	

Step 4a: Probability that a foreign authority will successfully enforce the claim through the provider

Legal Basis considered for the following assessment:	Section 702 FISA, other FISA warrants such as business records, pen registers and trap and trace devices, EOP 12.333 (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.

Prerequisite for success	**Probability per case**	**Rationale**

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%	100%	*Both Microsoft and its subprocessors (see recent list Nov 2021) may have access to Support Data data in plain tekst*
	... and is able to search for, find and copy the data requested by the authority (prerequisite no. 3)	100%			*Both Microsoft and its subprocessors (see recent list Nov 2021) may have access to Support Data in plain tekst*
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)	50%	50,00%		*By its nature, Support Data may be accessible to employees through admin priviliges.*
	... and are then able to search for, find and copy the data requested by the authority (prerequisite no. 3)	100%			*Idem*
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*
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)	50%		50%	*Speculative estimate, Microsoft lacks historical data on such scenarios and cannot provide a fact based rationale.*
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%	*All sub-processors are obligated by contract to redirect to Microsoft any third-party requests for Customer Data. As data importer Microsoft Corporation implements strict technical and organisational measures to protect access to the Security Data. 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 it 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 unduely access the Support 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)	80%		80%	*If Microsoft receives a valid order/warrant or subpoena, Microsoft may be subjected to gagging order and not permitted to inform its Customer. Hence Microsoft may not be in a position to issue a timely warning to its customer that it can no longer comply with the data protection guarantees in the SCC.*
Residual risk of successful lawful access by a foreign authority through the provider (given the countermeasures):				8,00%	
Step 4b: Probability of foreign lawful access by mass surveillance contents					
Legal Basis considered for the following assessment:		Section 702 US Foreign Intelligence Surveillance Act (FISA), Executive Order (EO) 12333			
		Probability in the period			**Rationale**
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%	0,00%	*The probability is zero for support tickets transferred to Microsoft in the USA, or its subprocessors, due to TLS encryption and the fact that the viewing of the data takes place within Microsoft's own secured environment.*
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%			*Idem*
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 certain recipients or senders of electronic communications) without the customer's permission as part of a downstream monitoring of online communications	0%	0,00%		*Idem*
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	0%			*Idem*
e)	Probability that the data is regarded as content that is the subject of intelligence searches in the country as per the above laws	5%			*It is not very plausible that support tickets sent to Microsoft by an EU gov or university organisation are considered interesting for intelligence searches, but it cannot be excluded*
Residual risk of successful lawful access by a foreign intelligence service without any guarantee of legal recourse (in view of the countermeasures):				0,00%	
Step 5: Overall assessment					
Probability that the question of lawful access via the cloud provider will arise at all (1 case in the period = 100%)				0,00%	
Probability of successful lawful access by the foreign authorities concerned in these cases despite the countermeasures				8,00%	
Probability of additional successful lawful access by a foreign intelligence service where there is no guarantee of legal recourse (despite countermeasures)				0,00%	
Overall probability of a successful lawful access to data in plain text via the cloud provider in the observation period:				0,00%	
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.pmi.org/learning/library/describing-probability-limitations-natural-language-7556).*					
Step 6: Data subject risks					
					Rationale
a)	*Estimated probability of occurance of successful lawful access risk:*	*0,00%*	*Very Low*		
b)	*Estimated impact of risk*	*3= regular personal data in the clear*	*High*		*Support Tickets may include special categories of data, and these data can be accessed in the clear by Microsoft employees in third countries, when necessary to solve the ticket. This DTIA assumes admins will follow the recommendation from SLM Rijk NOT to include any non-pseudonymised personal data in support tickets*

Very High	Low	High	High	High	High	*Low*
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	

Step 7: Define the safeguards in place		
		Rationale

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*		*By the end of 2022 all support tickets from EU Enterprise and Education customers will be processed within the EU, upon completion of Microsoft's EU data boundary. This 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)?	Yes	*Make sure that the prerequisites are fulfilled!*		*Incidental transfers outside of the EU, in a support ticket transferred to the USA, that can be accessed by Microsoft employees in third countries (Serbia, China and India), according to a follow-the-sun model. By the end of 2022 Support will be part of the EU Data Boundary.*
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 non-pseudonymised and special categories of personal data in support tickets in 2022, as long as they may still be escalated outside of the EU. Additionally, all traffic over the internet to Microsoft 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. The data in support tickets are by nature accessible in the clear for the support employees that are permitted to work with Support Data. MIcrosoft employees and Microsoft (sub-processors) agents are required to take the provided training on data handling. The (sub-processing list) based agents can only view personal data in Microsofts Core Online Services via highly controlled workspaces. Access to pseudonymous diagnostic data is possible without the permission of the manager but subprocessors do not have acces to keys or lookup lists to attribute pseudonymized data to a specific individual. For Core Online Services, there is no standing access by Microsoft personnel to Customer Data and any required access is for a limited time. All subprocessors in the "contract staff" category perform labor force augmentation services where the personal data remains only in Microsoft facilities on Microsoft systems and subject to Microsoft policies and supervision. The use of subprocessors in this manner does not expose customers to any appreciable incremental risk of government requests for their data, because between the subprocessors and Microsoft, the data remains continuously in Microsoft possession, custody, and control (including without limitation subject to all technical and organizational measures defined and implemented by Microsoft).*
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:		**permitted**			
Final Step: Conclusion					
In view of the above and the applicable data protection laws, the transfer is:		**permitted**			Reassess at the latest by: X+2
					(or if there are any changes in circumstances)
This Transfer Impact Assessment has been made by:				Place, Date:	
SLM Rijk / PRIVACY COMPANY				**Signed:**	
				By:	[Government org X, University Y]