# Data Transfer Impact Assessment (DTIA) on the transfer to the USA of stored Content Data in Teams, SharePoint and OneDrive



## 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 centres in the EU |
| e) | Context and purpose of the transfer: | Universities and government organisations can use Microsoft cloud servers to store files in OneDrive and Sharepoint. When they store recordings and transcriptions of Microsoft Teams conversations, these are stored in the organisation's OneDrive. |
| f) | Categories of data subjects concerned: | employees/workers and students/pupils with professional Education or Enterprise Microsoft accounts, and external guests with consumer accounts or without accounts invited to join a call hosted by [University X/government organisation Y] |
| g) | Categories of personal data transferred: | Organisations can store any kind of personal data in files on OneDrive and SharePoint. Such files can include recorded or transcribed contents of communications via Teams, including text, sound, video, and image files. Chats, recordings and transcriptions from Teams may include Account Data. See the separate tab in this DTIA for Account Data. |
| h) | Sensitive personal data: | Content Data, especially the contents of communications, are considered highly sensitive. This may for example include 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). Files stored or shared via OneDrive may also include personal data relating to criminal convictions and offences or related security measures (Art. 10 GDPR). Additionally, Account Data may be considered confidential, if an employee works for a government organisation with a high level of sensitivity, or sensitive if it concerns a minor. |
| i) | Technical implementation of the transfer: | End users can store files, including Teams recordings and transcriptions, in Microsoft OneDrive. The data are automatically processed on Microsoft servers in the EU, but these data are accessible from the USA (by compelled wiretap). Microsoft has assured SLM Rijk it will never initiate a recording itself. |
| j) | Technical and organizational measures in place: | Organisations can encrypt files in common data formats with their own key, with Microsoft Double Key Encryhption. This tooling is not available for Teams recordings and transcriptions, but admins can encrypt these recordings with Bring Your Own Key. However, this does not offer the same protection as Double Key Encryption. The Customer Key is stored on Microsoft's cloud servers and Microsoft can (with difficulty) intercept or copy the key, and access the data in the clear. Additionally, admins can choose to enable Customer Lockbox. This tool blocks access to any data in Exchange Online, SharePoint and One Drive until the customer has approved. |
| k) | Relevant onward transfer(s) of personal data (if any): | Incidentally, only if a customer knowingly provides Content Data in a Support Request to Microsoft - See the tab Support Data TOS. 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 the 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 will ensure that Subprocessors are bound by written agreements that require them to provide at least the level of data protection required of Microsoft by the DPA, including the limitations on disclosure of Processed Data. Microsoft agrees to oversee the Subprocessors to ensure that these contractual obligations are met. |
| l) | Countries of recipients of relevant onward transfer(s): | N/a |

## 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 | | *Stored content Data must necessarily be made accessible for customers in the clear. If the customer cannot control his own key, but needs to store the key on Microsoft's cloud servers to decrypt the data when access is wanted, Microsfot can access the data in the clear. 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.* |
| 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** | 50% | 0,25 | | *Stored content Data must necessarily be made accessible for customers in the clear. If the customer cannot control his own key, but needs to store the key on Microsoft's cloud servers to decrypt the data when access is wanted, Microsfot can access the data in the clear. 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.* |
| 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% | 0,19 | | *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.* |
| 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 | *It is assumed this question tries to assess the probability that Microsoft is hacked. This cannot be excluded.* |
| 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 | | | | 0,04 | |

## 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 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.

| | 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) | 90% | 81,00% | 100% | *A customer can allow access in case of a specific support request, and lift any self-applied encryption and protection measures, including Customer LockBox. Additionally, Microsoft is capable of lifting encryption on files stored in OneDrive, even if encrypted with a Customer Key.* |
| | ... and is able to search for, find and copy the data requested by the authority (prerequisite no. 3) | 90% | | | *A customer can allow access in case of a specific support request, and lift any self-applied encryption and protection measures, including Customer LockBox. Additionally, Microsoft is capable of lifting encryption on files stored in OneDrive, even if encrypted with a Customer Key.* |
| 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 OneDrive files, including all Teams recordings, transcriptions and chats stored in OneDrive, if they are not protected with a key exclusively controlled by the customer (Double Key Encryption).* |
| | ... 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. Since Microsoft is a processor, not a controller, the chance is reduced to 50%.* |
| 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 data stored in SharePoint and OneDrive (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 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 stored Content 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 OneDrive files, including all Teams recordings, transcriptions and chats stored in OneDrive, if they are not protected with a key exclusively controlled by the customer (Double Key Encryption). 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): | | | | 10,00% | |
| | | | | | |
| **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) 12.333 | | | |
| | | | | | |
| | | **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% | | *TLS encryption, encryption of contents from Customer to Microsoft endpoint* |
| 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% | | | *TLS encryption, encryption of contents from Customer to Microsoft endpoint* |
| 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% | *TLS encryption, encryption of contents from Customer to Microsoft endpoint* |
| 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% | 0,00% | | *TLS encryption, encryption of contents from Customer to Microsoft endpoint* |
| 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 recordings and transcriptions made by an EU gov or university organisation are interesting for law enforcement and/or security services. Even if stored on EU servers, the data are accessible in clear text/can be decrypted 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% | |
| | | | | | |
| **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%) | | | | 3,75% | |
| Probability of successful lawful access by the foreign authorities concerned in these cases despite the countermeasures | | | | 10,00% | |
| 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:** | | | | 0,38% | |
| | | | | | |
| 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** | | | | | |
| | | | | | |
| *a)* | *Estimated probability of occurance of successful lawful access risk:* | *0,02%* | *Very Low* | | |
| *b)* | *Estimated impact of risk* | *4= special categories of data in the clear* | *Very High* | | |
| |  | | *High* | | *The Content Data stored on SharePoint and OneDrive (including recorded Teams conversations, chats, transcriptions) can include special categories of data. Organisations are advised not to store Teams recordings or files with such data in OneDrive, unless the data are already public (such as court hearings or university lectures).* ***If organisations only exchange 'regular' personal data in Teams and make cloud recordings of such conversations, and/or only store 'regular' personal data in SharePoint/OneDrive, use Customer Key and Customer Lockbox, and possibly use pseudonyms for employees whose identity should remain confidential, the risk of undue access to the stored content data, including Teams recordings and chats, is low.*** |
| | | | | | |
| **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* | | *Microsoft has anounced 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 | | | *Factually this involves incidental transfers when the data stored in the EU are accessed and decrypted by Microsoft employees in the USA or subprocessors. 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 in the 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, Microsoft has acces to the encryption keys, and can access cloud recording stored in OneDrive on its EU servers.* |
| 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 not make recordings or transcriptions of Teams conversations in which special categories of data are exchanged. They can make cloud recordings with 'regular' personal data in Teams and store these in OneDrive. They should use Customer Key/Customer Lockbox, and possibly use pseudonyms for employees whose identity should remain confidential.* |
| | | | | | |
| **Final Step: Conclusion** | | | | | |
| | | | | | |
| **In view of the above and the applicable data protection laws, the transfer is:** | | **not permitted** | | | |

| | | | | | |
|---|---|---|---|---|---|
| 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 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| This Transfer Impact Assessment has been made by: | | | Place, Date: | | | | |
| *SLM / PRIVACY COMPANY* | | | **Signed:** | | | | |
| | | | By: | [Government org X, University Y] | | | |