TRANSFER IMPACT ASSESSMENT

INTRODUCTION

Before personal data can be transferred to a third country, the double legal basis in GDPR must be respected; 1) The data exporter must have a legal basis for processing and 2) there must be established a legal transfer basis for the transfer. In the light of the Schrems II verdict of 16 July 2020 these requirements are however no longer sufficient. Now, it is also required to perform a concrete risk assessment of the transfer of personal data to a third country in order to ensure compliance with the four essential European guarantees.

Below, we have conducted a specific risk assessment of Microsoft and the third country transfer in question based on Microsoft's Data Processor Agreement: Data Protection Addendum for Microsoft Products and Services, updated September 15, 2022 ("Addendum", "Data Processor Agreement").

Risk Assessment Results:

Question	Comments
Data exporter	Actee ApS (“Data exporter”, “Client”)
Country of data exporter	Denmark
Data importer	Microsoft Corporation (“Dataimporter”, “Microsoft”, “Supplier”) One Microsoft Way, Redmond, WA 98052, USA
Service(s) delivered by the data importer:	Azure Cloud Service
Country of data importer:	USA
Basis of the transfer:	EU standard contractual clauses (SCC)
Date of validation	October 2022

Question	Comments
Which types of processing activities are carried out when personal data is processed?	Microsoft will use and otherwise process Customer Data, Professional Services Data, and Personal Data only as described and subject to the limitations provided below (a) to provide Customer the Products and Services in accordance with Customer's documented instructions and (b) for business operations incident to providing the Products and Services to Customer. (cf. Nature of Data Processing: Ownership pp. 5). For purposes of this DPA, "to provide" a Product consists of: • Delivering functional capabilities as licensed, configured, and used by Customer and its users, including providing personalized user experiences. • Troubleshooting (preventing, detecting, and repairing problems); and • Keeping Products up to date and performant, and enhancing user productivity, reliability, efficacy, quality, and security. For purposes of this DPA, "to provide" Professional Services consists of: • Delivering the Professional Services, including providing technical support, professional planning, advice, guidance, data migration, deployment, and solution/software development services. • Troubleshooting (preventing, detecting, investigating, mitigating, and repairing problems, including Security Incidents and problems identified in the Professional Services or relevant Product(s) during delivery of Professional Services); and • Enhancing delivery, efficacy, quality, and security of Professional Services and the underlying Product(s) based on issues identified while providing Professional Services, including fixing software defects and otherwise keeping Products and Services up to date and performant. (cf. processing to Provide Customer the Products and Services, pp. 6). For purposes of this DPA, "business operations" means the processing operations authorized by customer in this section. Customer authorizes Microsoft: (i.) to create aggregated statistical, non-personal data from data containing pseudonymized identifiers (such as usage logs containing unique, pseudonymized identifiers); and (ii.) to calculate statistics related to Customer Data or Professional Services Data in each case without accessing or analyzing the content of Customer Data or Professional Services Data and limited to achieving the purposes below, each as incident to providing the Products and Services to Customer. Those purposes are: (1) billing and account management, (2) compensation such as calculating employee commissions and partner incentives, (3) internal reporting and business modeling, such as forecasting, revenue, capacity planning, and product strategy,

	and (4) financial reporting. (cf. Processing for Business Operations Incident to Providing the Products and Services to Customer, pp. 6) When processing for these business operations, Microsoft will apply principles of data minimization and will not use or otherwise process Customer Data, Professional Services Data, or Personal Data for: (a) user profiling, (b) advertising or similar commercial purposes, or (c) any other purpose, other than for the purposes set out in this section. In addition, as with all processing under this DPA, processing for business operations remains subject to Microsoft's confidentiality obligations and commitments under Disclosure of Processed Data. (cf. Processing for Business Operations Incident to Providing the Products and Services to Customer, pp. 6). To the extent Microsoft uses or otherwise processes Personal Data subject to the GDPR for business operations incident to providing the Products and Services to Customer, Microsoft will comply with the obligations of an independent data controller under GDPR for such use. (cf. Processor and Controller Roles Responsibilities, pp. 7). Hereby it can be inferred that Microsoft also processes personal data for its own purposes and acts as a data controller.
What types of personal is processed?	The types of Personal Data processed by Microsoft when providing the Products and Services include: (i) Personal Data that Customer elects to include in Customer Data and Professional Services Data; and (ii) those expressly identified in Article 4 of the GDPR that may be generated, derived or collected by Microsoft, including data sent to Microsoft as a result of a Customer's use of service-based capabilities or obtained by Microsoft from locally installed software. The types of Personal Data that Customer elects to include in Customer Data and Professional Services Data may be any categories of Personal Data identified in records maintained by Customer acting as controller pursuant to Article 30 of the GDPR, including the categories of Personal Data set forth in Appendix B. (cf. Processing Details, pp. 7). "Customer Data" means all data, including all text, sound, video, or image files, and software, that are provided to Microsoft by, or on behalf of, Customer through use of the Online Service. Customer Data does not include Professional Services Data. "Professional Services Data" means all data, including all text, sound, video, image files or software, that are provided to Microsoft, by or on behalf of a Customer (or that Customer authorizes Microsoft to obtain from a Product) or otherwise obtained or processed by or on behalf of Microsoft through an engagement with Microsoft to obtain Professional Services. (cf. Definitions, pp. 4).

What are the categories of the data subjects?	The data exporters employees, customers, and partners. The categories of data subjects are Customer's representatives and end users, such as employees, contractors, collaborators, and customers, and may include any other categories of data subjects as identified in records maintained by Customer acting as controller pursuant to Article 30 of the GDPR, including the categories of data subjects set forth in Appendix B. (cf. Processing Details, pp. 7).

Question	Mark with an x						Comments
Has a data processor agreement been concluded?	Yes	X	No		Don't know		
Is personal data transferred to a country outside the EU/EEA?	Yes	X	No		Don't know		USA or another country where Microsoft or its sub-processors do business. (cf. Data Transfers, pp. 9)
Has a transfer basis been established?	Yes	X	No		Don't know		Standard Contractual Clauses (SCC) (cf. Data Transfers, pp. 9)
Is personal data stored outside the EU/EEA?	Yes		No	X	Don't know		
Is personal data transferred when the Supplier carries out technical security measures?	Yes		No		Don't know	X	It is described that data transfers take place in the following cases: Considering such safeguards, Customer appoints Microsoft to transfer Customer Data, Professional Services Data, and Personal Data to the United States or any other country in which Microsoft or its Subprocessors operate and to store and process Customer Data, and Personal Data to provide the Products, except as described elsewhere in the DPA Terms (cf. Data Transfers, pp. 9). For purposes of this DPA, "to provide" a Product consists of: • Delivering functional capabilities as licensed, configured, and used by Customer and its users, including providing personalized user experiences. • Troubleshooting (preventing, detecting, and repairing problems); and • Keeping Products up to date and performant, and enhancing user productivity, reliability, efficacy, quality, and security. Therefore, it cannot be excluded that personal data are transferred when the Supplier carries out technical security measures.

Is personal data transferred when the Supplier carries out support?	Yes	X	No	Don't know	It is described that data transfers take place in the following cases: Taking into account such safeguards, Customer appoints Microsoft to transfer Customer Data, Professional Services Data, and Personal Data to the United States or any other country in which Microsoft or its Subprocessors operate and to store and process Customer Data, and Personal Data to provide the Products, except as described elsewhere in the DPA Terms. (cf. Data Transfers, pp. 9). For purposes of this DPA, "to provide" a Product consists of: • Delivering functional capabilities as licensed, configured, and used by Customer and its users, including providing personalized user experiences; • Troubleshooting (preventing, detecting, and repairing problems); and • Keeping Products up to date and performant, and enhancing user productivity, reliability, efficacy, quality, and security. Since product means troubleshooting, including the elimination of problems, it must be assumed that the transfer of per-protocol data occurs or may occur in the performance of support.

Question	Mark with an x						Comments
THE FOUR ESSENTIAL EUROPEAN GURANTEES							
Does the legislation in the third country provide a level of protection that is essentially equivalent to the level of protection in the EU/EEA?	Yes		No	x	Don't Know	X	The US legislation does not meet the proportionality requirements of EU/EEA law in case of interference with fundamental human rights and the (European) data subjects do not have the right to effective judicial remedies, which is among the four essential European guarantees. However, the data exporter as well as the data importer have implemented additional measures, including technical measures, beyond the established transfer tool in the form of the 2021 Standard Contractual Clauses (SCC), to ensure data security and to protect data subjects. These implemented additional measures attempt to address the problematic legislation in the U.S. The US system does not currently comply with the European standards for the processing of personal data, which results in some uncertainty. However, on October 7, 2022, the US announced and signed an executive and related Regulations implementing the agreement in principle announced in March on a new EU-US data protection framework. The executive order introduces new binding security safeguards to limit the access to EU data by US intelligence services and an establishment of an independent and impartial redress mechanism, which includes a new Data Protection Review Court ('DPRC'). This are significant improvements compared to the Privacy Shield - and are approaching European standards. The uncertainty concerning the processing of personal data is thereby met. However, the new system in the US must be approved by the EU Commission. The approval process is expected to take 4 to 6 months.
Does the law of the third country allow intelligence services or other authorities to access	Yes	X	No		Don't Know		FISA 702 authorizes the U.S. government to obtain information about "non-U.S. persons" who may reasonably be expected to be outside the United States for the purpose of collecting

Question	Mark with an x			Comments
personal data to a greater extent than what is necessary and proportionate?				"foreign intelligence information." This is done by issuing directives to "electronic communications service providers" to disclose or cause to be disclosed personal information that the provider processes. Cloud providers are typically considered as "electronic communications service providers". The uncertainty concerning the processing of personal data is being addressed, cf. the field above.
Will the data exporter be informed by the data importer if authorities of the third country gain access to the transferred personal data?	Yes	X*	No	Don't know	The data exporter will be notified in the following cases. * However, there may be cases where Microsoft is prevented from providing such notification. Microsoft will not disclose or provide access to any Processed Data to law enforcement unless required by law. If law enforcement contacts Microsoft with a demand for Processed Data, Microsoft will attempt to redirect the law enforcement agency to request that data directly from Customer. If compelled to disclose or provide access to any Processed Data to law enforcement, Microsoft will promptly notify Customer and provide a copy of the demand unless legally prohibited from doing so. (cf. Disclosure of Processed Data, pp. 6). See also clause 15 in the standard contract clauses from 2021: *15.1 Notification* *(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it: (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the*

Question	Mark with an x	Comments
		personal data requested, the requesting authority, the legal basis for the request and the response provided; or (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer. [For Module Three: The data exporter shall forward the notification to the controller.] *(b) If the data importer is prohibited from notifying the data exporter and/or the data* *subject under the laws of the country of destination, the data importer agrees to use* *its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the* *data exporter.* *(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). [For Module Three: The data exporter shall forward the information to the controller.]* *(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request. (e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.*

Question	Mark with an x						Comments
Is there an independent and effective supervisory authority in the third country?	Yes	(x)	No	X	Don't know		Please see the description of the new EU-U.S. Data Privacy Framework and the Executive Order from October 2022 above.
Are there available and effective remedies for the data subjects in the third country?	Yes	(x)	No	X	Don't know		Please see the description of the new EU-U.S. Data Privacy Framework and the Executive Order from October 2022 above.
ADDITIONAL SECURITY MEASURES							
TECHNICAL MEASURES							
Is personal data stored encrypted?	Yes	X	No		Don't know		• Customer Data and Professional Services Data (each including any Personal Data therein) in transit over public networks between Customer and Microsoft, or between Microsoft data centers, is encrypted by default. • Microsoft also encrypts Customer Data stored at rest in Online Services and Professional Services Data stored at rest. In the case of Online Services on which Customer or a third-party acting on Customer's behalf may build applications (e.g., certain Azure Services), encryption of data stored in such applications may be employed at the discretion of Customer, using either capabilities provided by Microsoft or obtained by Customer from third parties (cf. Data Encryption, pp. 8). • Microsoft encrypts, or enables Customer to encrypt, Customer Data and Professional Services Data that itransmitted over public networks. Microsoft restricts access to Customer Data and Professional Services Data in media leaving its facilities.(cf. Communication and Operations Management, pp. 13)
Does the data importer have access to the encryption key?	Yes		No		Don't know	X	It must be assumed that Microsoft holds the encryption key, as the following is described in the Data Processor Agreement: Microsoft will not provide any third party: (a) direct, indirect, blanket, or unfettered access to Processed Data; (b) platform encryption keys used to secure Processed Data or the ability to break such encryption; or (c) access to Processed Data if Microsoft is aware that the data is to be used for purposes other than those stated in the third party's request.

Question	Mark with an x					Comments
						In support of the above, Microsoft may provide Customer's basic contact information to the third party. (cf. Disclosure of Processed Data, pp. 6)
Is personal data subject to pseudonymization?	Yes		No	Don't know	X	In the Data Processor Agreement Annex 1 - Terms of the EU General Data Protection Regulation, page 19-20, it is described that Microsoft and the Customer will implement technical and organizational measures to ensure a suitable level of security in relation to the risk, including among others: (a) pseudonymization and encryption of Personal Data However, it is not clear whether Microsoft or Customer carries out this task.
Does the data importer log all its processing of personal data?	Yes	X	No	Don't know		• Microsoft logs data restoration efforts, including the person responsible, the description of the restored data and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process. (cf. Communication and Operations Management, p. 13) • Microsoft logs, or enables Customer to log, access and use of information systems containing Customer Data or Professional Services Data, registering the access ID, time, authorization granted or denied, and relevant activity (cf. Communication and Operations Management, pp. 13)
Are there other technical measures that have been implemented?	Yes	X	No	Don't know		See Appendix A – Technical measurements
ORGANISATIONAL MEASURES						
Has the data importer implemented processes and politics for documentation of request from authorities for disclosure of personal data?	Yes	X	No	Don't know		Microsoft will not disclose or provide access to any Processed Data to law enforcement unless required by law. If law enforcement contacts Microsoft with a demand for Processed Data, Microsoft will attempt to redirect the law enforcement agency to request that data directly from Customer. If compelled to disclose or provide access to any Processed Data

Question	Mark with an x				Comments
					to law enforcement, Microsoft will promptly notify Customer and provide a copy of the demand unless legally prohibited from doing so (cf. Disclosure of Processed Data, pp. 6) See also clause 15.1 (d) in the standard contract clauses from 2021 (SCC): *(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.*
Is it possible for the data exporter to get access to or receive records from the data importer regarding 1) authorities' requests for disclosure of personal data and 2) information on what personal data that has been handed over to the authorities?	Yes	X*	No	Don't know	The data exporter will be notified and receive information in the following cases. * However, there may be cases where Microsoft is prevented from providing such notification. See below from the Data Processing Agreement regarding claims from police authorities: Microsoft does not disclose or provide access to Processed Data to law enforcement, except as required by law. If a law enforcement agency contacts Microsoft with a request to provide Processed Data, Microsoft will attempt to have the law enforcement agency obtain such data directly from the customer. If we are required to disclose or provide access to Processed Data to law enforcement, Microsoft will immediately notify the Customer and provide a copy of the request, unless we are legally prohibited from doing so. (cf. Disclosure of Processed Data, p. 6) See also article 15.1 the Standard Contractual Clauses 2021 (SCC), as mentioned above.
Are the process and policies based on EU certifications or other international standards	Yes	X	No	Don't know	Microsoft will implement and maintain appropriate technical and organizational measures to protect Customer Data, Professional Services Data, and Personal Data against accidental

Question	Mark with an x					Comments
(e.g. ISO-norms) implemented by the data importer?						or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. Those measures shall be set forth in a Microsoft Security Policy. Microsoft will make that policy available to Customer, along with other information reasonably requested by Customer regarding Microsoft security practices and policies. In addition, those measures shall comply with the requirements set forth in ISO 27001, ISO 27002, and ISO 27018. A description of the security controls for these requirements is available to Customers. (cf. Security Practices and Policies, pp. 8)
Does the data importer regularly review in-ternal processes and policies to assess the adequacy of the implemented additional security measures?	Yes		No	Don't know	X	The Data Processor Agreement Annex 1 - Terms of the EU General Data Protection Regulation, page 19-20, point 4(d), it is described that the Customer and Microsoft implement technical and organisational measures to ensure an appropriate le vel of security in relation to the risks, including, among others: (d) a process for periodically testing, assessing, and evaluating the effectiveness of the technical and organizational measures to ensure the security of the data processing (Article 32(1)). However, it is not clear whether Microsoft or the Customer is carrying out this task.
Are other organisational measures implemented?	Yes	X	No	Don't know		Se Appendix A – Technical measurements.
CONTRACTUAL MEASURES						
Are specific technical measures required according to the contract concluded with the data importer?	Yes	X	No	Don't know		In particular the Data Processor Agreement Appendix A and Annex 1 - Terms of the EU General Data Protection Regulation.
Has a contract been concluded with the data importer, which requires that the level of protection has to be essentially equivalent to the level of protection in the EU/EEA?	Yes	(X)	No	Don't know		This is not directly stated in the data processor agreement. However, the following is stated:

Question	Mark with an x					Comments
						Microsoft is compliant with all laws and regulations applicable to the delivery of the Products and Services, including the Security Breach Information Act and Data Protection Requirements (cf. Regulatory Compliance, p. 5).
Has a contract been concluded with the data importer, which requires that the data importer may not make changes to their handling (e.g. technical security measures) of personal data in such a way that it becomes easier to access personal data?	Yes		No	X	Don't know	
Has a contract been concluded with the data importer, which requires that the data im-porter is not allowed to have" back-doors", which can provide for example authorities easier access to personal data?	Yes		No	X	Don't know	However, the following process has been implemented for requests from authorities as described above: Microsoft will not disclose or provide access to any Processed Data to law enforcement unless required by law. If law enforcement contacts Microsoft with a demand for Processed Data, Microsoft will attempt to redirect the law enforcement agency to request that data directly from Customer. If compelled to disclose or provide access to any Processed Data to law enforcement, Microsoft will promptly notify Customer and provide a copy of the demand unless legally prohibited from doing so. (cf. Disclosure of Processed Data, p. 6)
Has a contract been concluded with the data importer, which sets requirements for carry-ing out an audit, including the preparation of an audit report?	Yes	X	No		Don't know	In particular section: Compliance with Microsoft Audit Report, which states that Microsoft makes an audit report available on their Trustsite.
Has a contract been concluded with the data importer, that contains a list of laws, rules and case law which can give authorities access to the transferred personal data?	Yes		No	X	Don't know	
Has a contract been concluded with the data importer, where the data importer is obliged to assess the legality of all disclosures of personal data to authorities before a disclosure thereof takes place?	Yes	X	No		Don't know	Cf. below from the Data Processing Agreement regarding disclosure of processed data: Microsoft does not disclose or provide access to Processed Data except: (1) as directed by Customer; (2) as described in this Data Protection Addendum; or (3) as required by law. For purposes of

Question	Mark with an x	Comments
		this section, "Processed Data" means: (a) Customer Data; (b) Professional Services Data; (c) Personal Information; and (d) any other data processed by Microsoft in connection with the Products and Services that is Customer Confidential Information under the Volume License Agreement. All processing of Processed Data is subject to Microsoft's confidentiality obligation under the Volume License Agreement. Microsoft will not disclose or provide access to processed data to law enforcement, except as required by law. If a law enforcement agency contacts Microsoft with a request to provide Processed Data, Microsoft will attempt to have the law enforcement agency obtain such data directly from Customer. If we are required to disclose or provide access to Processed Data to law enforcement, Microsoft will immediately notify Customer and provide a copy of the request, unless we are legally prohibited from doing so. Microsoft will disclose or provide access to Processed Data only as required by law, provided that such laws and practices respect fundamental rights and freedoms and do not exceed what is necessary and appropriate in a democratic society to protect one of the purposes set out in Article 23(1) in the GDPR. Microsoft will disclose or provide access to Processed Data only as required by law, provided that such laws and practices respect fundamental rights and freedoms and do not exceed what is necessary and appropriate in a democratic society to protect one of the purposes set out in Article 23(1) in the GDPR. If Microsoft receives a request from a third party for processed data, Microsoft will notify the Customer immediately, unless we are legally prevented from doing so. Microsoft will reject the request unless compliance is required by law. If the request is valid, Microsoft will attempt to redirect the third party to request the data directly from the Customer.

Question	Mark with an x	Comments
		Microsoft will not provide to the third party: (a) direct, indirect or unfettered access to Processed Data; (b) platform encryption keys to protect Processed Data or the ability to break such encryption; or (c) access to Processed Data if Microsoft knows that the data will be used for purposes other than those specified in the third-party request. As a result of the above, Microsoft may provide Customer's basic contact information to the third party. (cf. Disclosure of Processed Data, pp. 6 and art. 15.2(a) and (b) i the Standard Contractual Clauses (SCC) from 2021: 15.2 Legality checks and data minimisation *(a) The Data Importer agrees to review the lawfulness of the request for disclosure of data, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if the Data Importer concludes, after a thorough assessment, that there are reasonable grounds to believe that the request is unlawful under the law of the destination country, applicable obligations under international law and the principles of international understanding. Under the same conditions, the data importer shall make use of the possibilities of appeal. When contesting a request, the data importer shall request interim measures to suspend the effects of the request until the competent judicial authority has decided on the merits of the case. The data importer shall first transmit the personal data requested in accordance with the applicable rules of procedure. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).*

Question	Mark with an x						Comments
							(b) The data importer agrees to document its legal assessment and any challenge to the data transfer request and make the documentation available to the data exporter to the extent permitted by the law of the country of destination. The data importer shall also make the documentation available to the competent supervisory authority upon request. [To module three: The data exporter makes the assessment available to the data controller].
Has a contract been concluded with the data importer, where the data importer is obliged only to provide the necessary personal data corresponding to the order to which the da-ta importer is subject by national law?	Yes	X	No		Don't know		See clause 15.2(c) of the Standard Contractual Clauses (SCC) from 2021: *(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.*
Er der indgået en kontrakt med Leverandøren, som sikrer en kort opsigelsesperiode, såfremt det viser sig, at tredjelandsoverførslen ikke er lovlig?	Yes	X	No		Don't know		Please see clause 16 of the Standard Contractual Clauses (SCC) from 2021.
Has a contract been concluded with the data importer, which ensures a short notice peri-od if it turns out that the third country trans-fer is not legal?	Yes	X*	No		Don't know		The data exporter will be notified in the following cases. * However, there may be cases where Microsoft is prevented from providing such notification. See the Standard Contractual Clauses (SCC) from 2021 as described below and the procedure on pp. 6 of the section "Disclosure of Processed Data" as described above. Please see also clause 15 of the 2021 Standard Contractual Clauses (SCC), described above.
Has a contract been concluded with the data importer, where the data importer is obliged to notify the data exporter of a request for access to personal data?	Yes		No	X	Don't know		Please see clause 10 of the Standard Contractual Clauses (SCC) from 2021.

Question	Mark with an x					Comments
Has a contract been concluded with the data importer, where the data importer is obliged to assist the data subject in regard to the exercise of their rights in the third country?	Yes	X	No		Don't know	Please see clause 10 of the Standard Contractual Clauses (SCC) from 2021.
Have other contractual measures been implemented?	Yes	X	No		Don't know	Please see the Data Processor Agreement and the Standard Contractual Clauses (SCC) from 2021.

Appendix A – Security Measures

Microsoft has implemented and will maintain for Customer Data in the Core Online Services and Professional Services Data the following security measures, which in conjunction with the security commitments in this DPA (including the GDPR Terms), are Microsoft's only responsibility with respect to the security of that data.

Domain	Practices	
Organization of Information Security	**Security Ownership.** Microsoft has appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures. **Security Roles and Responsibilities.** Microsoft personnel with access to Customer Data or Professional Services Data are subject to confidentiality obligations. **Risk Management Program.** Microsoft performed a risk assessment before processing the Customer Data or launching the Online Services service and before processing Professional Service Data or launching the Professional Services. Microsoft retains its security documents pursuant to its retention requirements after they are no longer in effect.	
Asset Management	**Asset Inventory**. Microsoft maintains an inventory of all media on which Customer Data or Professional Services Data is stored. Access to the inventories of such media is restricted to Microsoft personnel authorized in writing to have such access. **Asset Handling** - Microsoft classifies Customer Data and Professional Services Data to help identify it and to allow for access to it to be appropriately restricted. - Microsoft imposes restrictions on printing Customer Data and Professional Services Data and has procedures for disposing of printed materials that contain such data. - Microsoft personnel must obtain Microsoft authorization prior to storing Customer Data or Professional Services Data on portable devices, remotely accessing such data, or processing such data outside Microsoft's facilities.	
Human Resources Security	**Security Training**. Microsoft informs its personnel about relevant security procedures and their respective roles. Microsoft also informs its personnel of possible consequences of breaching the security rules and procedures. Microsoft will only use anonymous data in training.	

Domain	Practices	
Physical and Environmental Security	**Physical Access to Facilities**. Microsoft limits access to facilities where information systems that process Customer Data or Professional Services Data are located to identified authorized individuals. **Physical Access to Components**. Microsoft maintains records of the incoming and outgoing media containing Customer Data or Professional Services Data, including the kind of media, the authorized sender/recipients, date and time, the number of media and the types of such data they contain. **Protection from Disruptions**. Microsoft uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference. **Component Disposal**. Microsoft uses industry standard processes to delete Customer Data and Professional Services Data when it is no longer needed.	
Communications and Operations Management	**Operational Policy**. Microsoft maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Customer Data or Professional Services Data. **Data Recovery Procedures** - On an ongoing basis, but in no case less frequently than once a week (unless no updates have occurred during that period), Microsoft maintains multiple copies of Customer Data and Professional Services Data from which such data can be recovered. - Microsoft stores copies of Customer Data and Professional Services Data and data recovery procedures in a different place from where the primary computer equipment processing the Customer Data and Professional Services Data are located. - Microsoft has specific procedures in place governing access to copies of Customer Data and Professional Services Data. - Microsoft reviews data recovery procedures at least every six months, except for data recovery procedures for Professional Services and for Azure Government Services, which are reviewed every twelve months. - Microsoft logs data restoration efforts, including the person responsible, the description of the restored data and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process. **Malicious Software**. Microsoft has anti-malware controls to help avoid malicious software gaining unauthorized access to Customer Data and Professional Services Data, including malicious software originating from public networks.	

Domain	Practices	
	Data Beyond Boundaries - Microsoft encrypts, or enables Customer to encrypt, Customer Data and Professional Services Data that is transmitted over public networks. - Microsoft restricts access to Customer Data and Professional Services Data in media leaving its facilities. **Event Logging**. Microsoft logs, or enables Customer to log, access and use of information systems containing Customer Data or Professional Services Data, registering the access ID, time, authorization granted or denied, and relevant activity.	
Access Control	**Access Policy**. Microsoft maintains a record of security privileges of individuals having access to Customer Data or Professional Services Data. **Access Authorization** - Microsoft maintains and updates a record of personnel authorized to access Microsoft systems that contain Customer Data or Professional Services Data. - Microsoft deactivates authentication credentials that have not been used for a period of time not to exceed six months. - Microsoft identifies those personnel who may grant, alter or cancel authorized access to data and resources.	

Domain	Practices	
	- Microsoft ensures that where more than one individual has access to systems containing Customer Data or Professional Services Data, the individuals have separate identifiers/log-ins. **Least Privilege** - Technical support personnel are only permitted to have access to Customer Data and Professional Services Data when needed. - Microsoft restricts access to Customer Data and Professional Services Data to only those individuals who require such access to perform their job function. **Integrity and Confidentiality** - Microsoft instructs Microsoft personnel to disable administrative sessions when leaving premises Microsoft controls or when computers are otherwise left unattended. - Microsoft stores passwords in a way that makes them unintelligible while they are in force. **Authentication** - Microsoft uses industry standard practices to identify and authenticate users who attempt to access information systems. - Where authentication mechanisms are based on passwords, Microsoft requires that the passwords are renewed regularly. - Where authentication mechanisms are based on passwords, Microsoft requires the password to be at least eight characters long. - Microsoft ensures that de-activated or expired identifiers are not granted to other individuals. - Microsoft monitors, or enables Customer to monitor, repeated attempts to gain access to the information system using an invalid password. - Microsoft maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed. - Microsoft uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage.	

Domain	Practices	
	Network Design. Microsoft has controls to avoid individuals assuming access rights they have not been assigned to gain access to Customer Data or Professional Services Data they are not authorized to access.	
Information Security Incident Management	**Incident Response Process** - Microsoft maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data. - For each security breach that is a Security Incident, notification by Microsoft (as described in the "Security Incident Notification" section above) will be made without undue delay and, in any event, within 72 hours. - Microsoft tracks, or enables Customer to track, disclosures of Customer Data and Professional Services Data, including what data has been disclosed, to whom, and at what time. **Service Monitoring**. Microsoft security personnel verify logs at least every six months to propose remediation efforts if necessary.	
Business Continuity Management	- Microsoft maintains emergency and contingency plans for the facilities in which Microsoft information systems that process Customer Data or Professional Services Data are located. - Microsoft's redundant storage and its procedures for recovering data are designed to attempt to reconstruct Customer Data and Professional Services Data in its original or last-replicated state from before the time it was lost or destroyed.	