Microsoft

Compliance with EU transfer requirements for personal data in the Microsoft cloud

Compliance with EU transfer requirements for personal data in the Microsoft cloud

Contents

Summary

This paper provides guidance to customers of Microsoft Online Services and Professional Services (as defined in the Microsoft Products and Services Data Protection Addendum) in following the six steps the European Data Protection Board (EDPB) recommends that companies take to ensure adequate protection of personal data leaving the European Union (EU). For each step, the customer will find information about what Microsoft does, including a description of specific supplementary measures, to help support compliance with EDPB recommendations.

Introduction

On 16 July 2020, the Court of Justice of the European Union (CJEU) issued a ruling (known as "Schrems II") on transfers of personal data from the EU. The CJEU invalidated the EU-U.S. Privacy Shield but confirmed the continuing validity of the European Commission's Standard Contractual Clauses (SCC) as a legal transfer tool for personal data leaving the EU, provided there are sufficient supplemental safeguards. In response to this ruling, Microsoft stopped relying on the EU-U.S. Privacy Shield and continued its use of SCC as the lawful basis for personal data transfers. This enabled customers to continue to use Microsoft Online and Professional Services to move personal data from the EU.

Microsoft had anticipated the European Data Protection Board (EDPB) recommendations with its Defending Your Data initiative, which added a new contractual commitment to challenge all government requests for public sector and enterprise customer's personal data in cases where there is a lawful basis for doing so. The Defending Your Data commitment also provides for monetary compensation for customers' users if Microsoft were found to have disclosed their personal data in violation of GDPR transfer requirements.

Microsoft is committed to defending the principle that governments should never place global technology providers in the middle of state-on-state intelligence gathering or seeking of each other's public sector data held by the private sector.

Microsoft does not provide, and has never provided, EU public sector customer's personal data to any government.[1] Moreover, outside of the United States, Microsoft does not provide, and has never provided, EU enterprise customer's personal data to a jurisdiction that was not the same as that in which the enterprise was located in response to government demands for data.

In June 2021, the European Commission issued a set of modernized SCC to help companies lawfully transfer personal data from EU to non-EU countries that have not been deemed adequate as required under EU data protection law. Microsoft reviewed its practices in light of the new SCC, evaluated and adapted its supplementary measures, and on 15 September 2021, released an updated version of the Microsoft Products and Services Data Protection Addendum implementing the new SCC.

[1] For clarity, under U.S. law, providers can neither confirm nor deny having received any specific legal demands subject to a secrecy obligation. While Microsoft is obligated to comply with these restrictions in U.S. law, we disagree with them and continue to advocate for changes in the law to provide our customers and the public additional, important transparency. Please see our biannual U.S. National Security Report for the most comprehensive, legally permissible picture we can provide at this point of national security-related requests we receive from the U.S. government..

European Data Protection Board (EDPB) recommendations

In June 2021, the EDPB published a final version of its recommendations on supplementary measures that companies should implement to ensure adequate protection of personal data leaving the EU. It also confirmed that companies can use the SCC to continue to transfer personal data. These recommendations advise companies transferring personal data from the EU to focus on the practical risks of transfers in light of the data access laws and practices of destination countries outside the European Economic Area (EEA) and adequate jurisdictions outside the EU. The EDPB steps help ensure that personal data transfer tools do not impinge on the effectiveness of EU safeguards to protect personal data sent outside the EU.

There is an obligation on the data exporter (in Microsoft's case, Microsoft Ireland Operations Limited) and the importer of the personal data outside the EU (in Microsoft's case, the Microsoft Corporation) to make a risk-based assessment. They can do so by taking into account the circumstances of the transfer, including any supplementary measures that could be put in place. The types of supplementary measures (whether contractual, technical, or organizational) when transferring personal data to third countries should be assessed case by case.

European Data Protection Board (EDPB) recommendations (cont.)

The EDPB recommends data exporters take the following six steps to assess their personal data transfers and help them determine if they need to implement supplementary measures.

1. Map all transfers of personal data to third countries, and assess whether the data to be transferred is limited only to what is necessary.

2. Verify the transfer tool that will be used, such as the SCC.

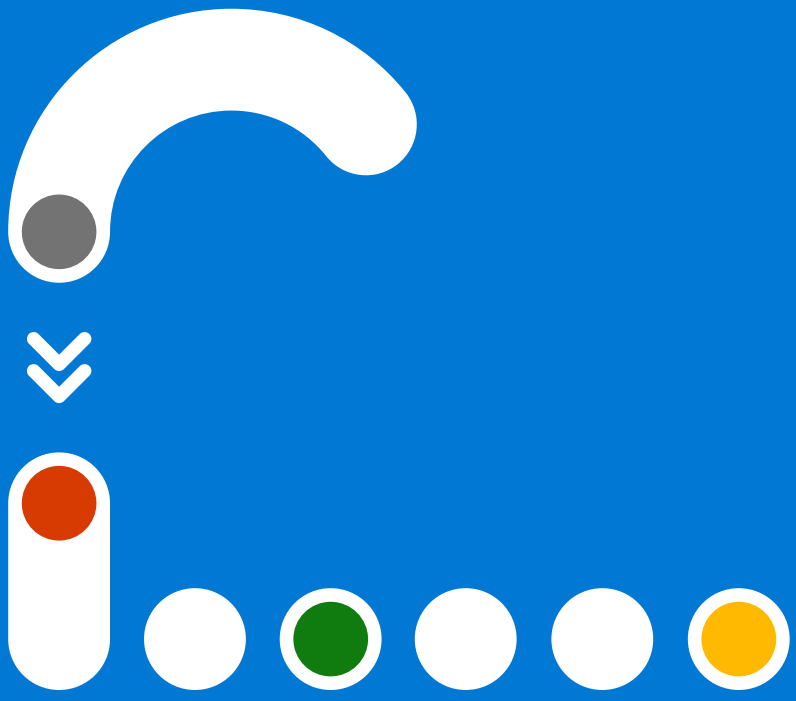
3. If relying on an Article 46 GDPR transfer tool, such as the SCC, assess whether it is effective in light of all circumstances of the transfer.

4. Identify and adopt supplementary measures—contractual, technical, and organizational—"that are necessary to bring the level of protection of the data transferred up to the EU standard of essential equivalence."

5. Take any formal procedural steps that the adoption of the supplementary measures may require.

6. Re-evaluate, when appropriate, the level of protection for personal data transferred to third countries, and monitor any developments that may affect the transfers.

Steps 1,2,3,4,5,6



Step 1. Mapping all transfers of personal data to third countries

The first step is to understand where all personal data goes so that when it is transferred outside the EU it is processed with a level of data protection that complies with EU law. In addition, data exporters need to assess whether the data to be transferred is limited only to what is necessary.

Microsoft offers customers various tools to specify where the personal data they provide to Microsoft through use of the services will be stored. Microsoft may also replicate to other regions for data resiliency. Customers and their users may move, copy, or access their data from any location globally.

Microsoft may transfer personal data out of the EU for processing, depending on the service in question. Microsoft offers a broad array of services, and data transfer processes and practices are specific to each service, as described in the following resources:

Azure Services:
Data Residency in Azure

Dynamics 365 and Power Platform:
Dynamics 365 and Power Platform availability

Microsoft 365:
Where your Microsoft 365 customer data is stored

Other Microsoft services:
Microsoft Privacy – Where your data is located, "Cloud services and data residency and transfer policies"

More information:

Enabling Data Residency and Data Protection in Microsoft Azure Regions

Step 2. Verifying the transfer tool

The second step is to verify the transfer tool which in the case of Microsoft services addressed in this document are the Standard Contractual Clauses (SCC) that were adopted by the European Commission in June 2021 and implemented by Microsoft in September 2021. Microsoft implemented the processor-to-processor module (module 3) of the SCC between Microsoft Ireland Operations Limited (as data exporter) and Microsoft Corporation (as data importer). The implementation of the 2021 SCC is reflected in the 15 September 2021 Microsoft Products and Services Data Protection Addendum.

More information

Microsoft Products and Services Data Protection Addendum

Microsoft 2021 Standard Contractual Clauses

Step 3. Assessing the laws or practices of the recipient country

The EDPB guidelines recommend that, in cases where personal data is transferred outside the EU, organizations consider the "practices in force in the third country" that bear on whether "in practice, the effective protection of the personal data" will be maintained. So, for Step 3, data exporters must assess if there is anything in the law or practice of the recipient country that may impinge on the safeguards of the transfer tools being used. Data exporters must also check for indications of practices in the country that are incompatible with EU law and the requirements of Article 46 of the GDPR regarding the transfer tool.

For this evaluation, Microsoft has assessed the publicly available information related to the laws and practices of destination countries outside the EU, EEA, and countries deemed adequate by the European Commission, along with safeguards put in place by Microsoft. Based on this assessment, Microsoft believes these laws and practices do not in practice prevent it from fulfilling its

Continued on next page

Step 3. Assessing the laws or practices of the recipient country (cont.)

obligations under the SCC in regards to transfers of personal data outside of the EU, and are compatible with commitments required by GDPR Article 46 regarding the transfer tools.

Given the focus of the Schrems II judgment, US law is particularly relevant. Microsoft Corporation, the data importer under the SCC, is a US entity with particular expertise and experience with requirements of US law. An analysis of relevant US law issues is attached as Annex 1: Microsoft Assessment Regarding the Practical Application of Section 702 and EO 12333.

Also, before opening (or considering opening) a data center in a new country, Microsoft conducts a rigorous assessment of local laws to validate that data in the country will be hosted in a manner that is consistent with Microsoft obligations to its customers.

Microsoft is committed to defending the principle that governments should never place global technology providers in the middle of state-on-state intelligence gathering or seeking of each other's public sector data held by the private sector. Microsoft does not provide, and has never provided, EU public sector customer's personal data to any government.[2]

Moreover, outside of the United States, Microsoft does not provide, and has never provided, EU enterprise customer's personal data to a jurisdiction that was not the same as that in which the enterprise was located in response to government demands for data.

More information

Annex 1: Microsoft Assessment Regarding the Practical Application of Section 702 and EO 12333

Microsoft Law Enforcement Requests Report

Microsoft U.S. National Security Orders Report

[2] For clarity, under U.S. law, providers can neither confirm nor deny having received any specific legal demands subject to a secrecy obligation. While Microsoft is obligated to comply with these restrictions in U.S. law, we disagree with them and continue to advocate for changes in the law to provide our customers and the public additional, important transparency. Please see our biannual U.S. National Security Report for the most comprehensive, legally permissible picture we can provide at this point of national security-related requests we receive from the U.S. government.

Step 4. Identifying supplementary protective measures

In the fourth step, data exporters need to identify supplementary measures that may be required to bring the level of protection of the personal data transferred up to the EU standard of "essential equivalence." Entities need to take this step only if their assessment in Step 3 reveals that the laws or practices of the destination country could negatively impact the effectiveness of the transfer tool. These measures fall into three categories: contractual, technical, and organizational.

Step 4.1 Contractual measures

In response to draft EDPB guidance, Microsoft bolstered its already strong protections for personal data of customers with new contractual language. Microsoft calls these protections Defending Your Data, and includes them in the Microsoft Products and Services Data Protection Addendum (DPA). These contractual commitments go beyond the law and EDPB recommendations in that they:

- Protect customer rights with every government request for public sector or enterprise customer's personal data—from any government—where there is a lawful basis for doing so.

- Provide monetary compensation to customer's users if Microsoft is found to have disclosed their personal data in response to a government request in violation of the requirements of the transfer tool, the SCC.

The above commitments are in addition to long-standing Microsoft contractual commitments made in the DPA to public sector and enterprise customers regarding requests for access to customers' data, including personal data, by third parties:

- No government has direct access to a customer's data, including personal data. Microsoft scrutinizes all government demands for legal validity and appropriateness. Microsoft has a proven track record of using the courts to challenge government demands that it believes are inappropriate and do not adhere to Microsoft commitments.

Continued on next page

Step 4.1 Contractual measures (cont.)

• Microsoft will not disclose or provide access to a customer's data to law enforcement unless required by law. If law enforcement contacts Microsoft with a demand for a customer's data, Microsoft will attempt to redirect the law enforcement agency to request that data directly from the customer. If compelled to disclose or provide access to any customer's data, including personal data, to law enforcement, Microsoft will promptly notify the customer and provide a copy of the demand unless legally prohibited from doing so.

• Upon receipt of any other third-party request for a customer's data, Microsoft will promptly notify the customer unless prohibited by law. Microsoft will reject the request unless required by law to comply. If the request is valid, Microsoft will attempt to redirect the third party to request the data directly from the customer.

• Microsoft will not provide any third party: (a) direct, indirect, blanket, or unfettered access to a customer's data, including personal data; (b) platform encryption keys used to secure a customer's data, including personal data, or the ability to break such encryption; or (c) access to a customer's data, including personal data, if Microsoft is aware that the data is to be used for purposes other than those stated in the third party's request.

More information

Microsoft Products and Services Data Protection Addendum, "Disclosure of Processed Data"

Step 4.2 Technical measures

Microsoft uses some of the strongest, most secure encryption protocols available as barriers against unauthorized access to enterprise and public sector Customer Data. Proper key management is also an essential element of encryption best practices, and Microsoft works to ensure that all Microsoft-managed encryption keys are well secured.

Continued on next page

Step 4.2 Technical measures (cont.)

- **Data encryption key management.**
Azure Key Vault provides powerful control over the management of data access. Azure Key Vault can be used to securely store and tightly control access to tokens, passwords, certificates, API keys, encryption keys, and other secrets.

- **Encryption in transit.**
Microsoft services use industry-standard secure transport protocols, such as Internet Protocol Security (IPsec) and Transport Layer Security (TLS), between Microsoft datacenters and between user devices and Microsoft datacenters.

- **Encryption at rest.**
Microsoft follows industry best practice including double encryption and service-level encryption; disk encryption protects the data stored in Microsoft datacenters. This defends against the highly unlikely possibility that someone gains physical access to a data storage device in a secure datacenter.

More information

Encryption in the Microsoft cloud

Azure encryption overview

Office 365 encryption

Encryption in Microsoft Dynamics 365

Compliance and data privacy - Power Platform

Step 4.3 Organizational measures

As the data importer, Microsoft Corporation implements robust organizational measures to protect transferred data, including information security, asset management, human resources security, physical and environmental security, operations management, access control, security incident management, and business continuity management. These measures

Continued on next page

Step 4.3 Organizational measures (cont.)

are set forth in the Microsoft Security Policy, and meet or exceed established industry standards for data security, including requirements in ISO/IEC 27001, ISO/IEC 27002, and ISO/IEC 27018.

Security roles and responsibilities: subprocessors

All personnel with access to Customer Data, Personal Data, or Professional Services Data are subject to confidentiality obligations.

When Microsoft engages other companies (subprocessors) to perform services in support of Microsoft Online Services and Professional Services, and these parties have access to personal data in the course of providing those services, all subprocessors are obligated by contract to redirect to Microsoft any third-party request for customer data.

Most subprocessors 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. There are no hosting locations other than those Microsoft already discloses, and these subprocessors do not have the independent ability to respond to government requests in the unlikely event they were to receive such requests.

Other subprocessors perform discrete functions in which they may process limited personal data on systems they control. While specifics vary with the particular scenario, technical controls help ensure that data protection consistent with Microsoft obligations to customers remains in place. Microsoft technology and delivery partners that process personal data on their own systems (such as Azure Databricks and Microsoft support call center service providers) may be legally compelled to independently disclose data in their possession.

Continued on next page

Step 4.3
Organizational measures (cont.)

However, these partners are limited in number, are required to maintain technical controls to ensure data protection consistent with Microsoft obligations to its customers, and are contractually obligated to provide Microsoft advance notice of any such third-party requests for personal data.

More information

Annex 2: Organizational supplementary protective measures implemented for Microsoft online services

Microsoft Online Services Subprocessor List

Microsoft Professional Services Suppliers

Step 5.
Taking procedural steps needed to adopt the supplementary measures

The fifth step is to take any formal procedural steps required by the supplementary measures the exporter has adopted.

Microsoft Ireland Operations Limited (as data exporter under the SCC) and Microsoft Corporation (as data importer) have ensured these measures support and do not contradict the SCC or the protections under the GDPR, and are thus effective supplementary measures.

Step 6.
Re-evaluating the level of protection for personal data

The last step is to re-assess at appropriate intervals the protection afforded to the personal data the data exporter has transferred to third countries and monitor any developments that have affected past data transfers or may impact transfers in the future.

Microsoft provides regular updates to the Data Protection Addendum and subprocessor lists. It also provides any needed updates to the technical and organizational measures outlined in the SCC. In addition, the Microsoft Security Response Center investigates all reports of security vulnerabilities affecting Microsoft products and services, and keeps customers informed of its efforts in the Security Update Guide.

More information

Microsoft Products and Services Data Protection Addendum (DPA)

Microsoft Online Services Subprocessor List

Microsoft Professional Services Suppliers

Microsoft Security Update Guide

Appendix
Annex 1

Annex 1: Microsoft Assessment Regarding the Practical Application of Section 702 and EO 12333

October 2021

Clause 14(a) of the Standard Contractual Clauses ("SCC") of June 4, 2021, requires both data exporters and importers to "warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorizing access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses." The SCC (cl. 14(b)) also require that, in making that assessment, the parties consider "the laws and practices of the third country of destination—including those requiring the disclosure of data to public authorities or authorizing access by such authorities . . . ."

In its Schrems II decision, the Court of Justice of the European Union concluded that Section 702 of the U.S. FISA Amendments Act ("Section 702") and U.S. Executive Order ("EO") 12333 do not provide EU data subjects with rights and remedies "essentially equivalent" to those provided under EU law. Consistent with the obligation under Clause 14 of the SCC, Microsoft has assessed whether it has reason to believe that Section 702 and/or EO 12333 would prevent Microsoft from fulfilling its obligations under the SCC. Having done this assessment, Microsoft has determined that it does not have reason to believe that these U.S. measures would prevent Microsoft from fulfilling its obligations under the SCC in the specific circumstances of the enterprise customer transfers contemplated here. In order to enable our enterprise customers to make their own assessment, we have set out below the factors that underpin our conclusion.

Section 702

Microsoft has reviewed relevant and reliable publicly available documents issued by U.S. Government authorities involved in or otherwise knowledgeable about the U.S. Government's use of Section 702 surveillance authorities, and thus has fulfilled the SCC requirement that it examine "the application of [Section 702] in practice." SCC, cl. 14 n.12. A list of those documents is included as Appendix A (collectively, the "Record"). Microsoft analyzed the information gleaned from the Record to generate insights into how the U.S. Government actually applies Section 702 authorities. Based on this review, Microsoft has drawn the following conclusions about the practical application of Section 702:

- The Record provides no reason to believe that, in practice, the U.S. Government uses Section 702 to target legitimate private enterprises. The vast majority of examples of Section 702's application set out in public sources involve the collection of data relating to the actions of individuals and/or criminal groups (e.g., terrorist networks). Although the Record reveals an example of Section 702 being used to collect information relating to an enterprise, this example involved a "front company" that was engaged in illegal weapons acquisition for a Middle East terrorist organization.

- The Record provides no reason to believe that, in practice, the U.S. Government targets European Economic Area ("EEA") governments with Section 702 data collection. Although the publicly available sources disclose several examples of Section 702 surveillance that uncovered and thwarted terrorist attacks in Europe, none of these sources references or even suggests any collection of data from governments located in the EEA.

- In practice, the Record indicates that the U.S. Government uses Section 702 primarily to collect information in aid of investigations of terrorism, cybersecurity attacks, and weapons proliferation. Section 702 is not used for industrial espionage or to otherwise further U.S. commercial interests.

- A multi-layer oversight mechanism—involving all three branches of the U.S. Government, including the Foreign Intelligence Surveillance Court ("FISC"), Congress, the Department of Justice ("DOJ"), the Office of the Director of National Intelligence ("ODNI"), and independent Inspectors General of relevant national security agencies—is designed to ensure that Section 702 authorities are applied lawfully and are being operationalized in a manner consistent with U.S. law and policy commitments. For example, this oversight mechanism is designed to ensure that Section 702 is used only to gather specific categories of foreign intelligence information following clearly delineated targeting, minimization, and querying procedures, all of which must be approved by the FISC. Data may be collected only about individual targets, with targeting decisions reviewed by several agencies, including the National Security Agency, DOJ, and ODNI.

Accordingly, based on its comprehensive assessment of the Record, Microsoft concludes that it has no reason to believe that Section 702 would prevent Microsoft from fulfilling its obligations under the SCC in the specific circumstances of the transfers involved here.

EO 12333

EO 12333 authorizes elements of the U.S. Intelligence Community to collect foreign intelligence information and regulates intelligence collection techniques conducted by the U.S. Intelligence Community. However, unlike Section 702, EO 12333 does not permit the U.S. Government to compel private parties to disclose information. Accordingly, the U.S. Government's principal means of collection under EO 12333 are (1) voluntary cooperation by private parties, and (2) technical collection when private party assistance is not needed.

Microsoft will not comply with any request issued under EO 12333. Moreover, Microsoft encrypts customer data in transit, to include data transferred between the EEA and U.S., which we believe to be an effective safeguard against data collection under EO 12333 without Microsoft's cooperation.

In light of the above, Microsoft concludes that it has no reason to believe that EO 12333 would prevent Microsoft from fulfilling its obligations under the SCCs in the specific circumstances of the transfers involved here.

Appendix A: Record for Section 702 Assessment

Appendix A: The following publicly available sources were reviewed and analyzed to produce the Section 702 Assessment.

Executive & Legislative Branch

- Off. of the Dir. of Nat'l Intel., Annual Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Surveillance Authorities: Calendar Year 2020 (Apr. 2021) (here).
- Cong. Rsch. Serv., Foreign Intelligence Surveillance Act (FISA): An Overview (Apr. 6, 2021) (here).
- Dept. of Com., Dept. of Just., Off. of Dir. of Nat'l Intel., Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers After Schrems II, White Paper (Sept. 2020) (here).
- Off. of the Dir. of Nat'l Intel., Statistical Transparency Report Regarding the Use of National Security Surveillance Authorities: Calendar Year 2019 (Apr. 2020) (here).
- Dept. of Just. & Off. of the Dir. of Nat'l Intel., Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Reporting Period: June 1, 2017-Nov. 30, 2017 (Dec. 2019) (here).
- Off. of the Dir. of Nat'l Intel., Statistical Transparency Report Regarding the Use of National Security Surveillance Authorities: Calendar Year 2018 (Apr. 2019) (here).
- Dept. of Just. & Off. of the Dir. of Nat'l Intel., Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Reporting Period: Dec. 1, 2016-May 31, 2017 (Oct. 2018) here).
- Off. of the Dir. of Nat'l Intel., Statistical Transparency Report Regarding the Use of National Security Surveillance Authorities: Calendar Year 2017 (Apr. 2018) (here).
- Nat'l Sec. Agency, "Section 702" Saves Lives, Protects the Nation and Allies (Dec. 12, 2017) (here).
- Off. of the Dir. of Nat'l Intel., Guide to Section 702 Value Examples (Dec. 4, 2017) (here).
- Off. of the Dir. of Nat'l Intel., Protecting U.S. Person Identities in Disseminations under the Foreign Intelligence Surveillance Act (Nov. 2017) (here).
- Nat'l Sec. Agency, An Illustration: Understanding the Impact of Section 702 on the Typical American (Nov. 17, 2017) (here).
- Glenn S. Gerstell, General Counsel, Nat'l Sec. Agency, Speech: Judicial Oversight of Section 702 of the Foreign Intelligence Surveillance Act (Sept. 14, 2017) (here).
- Nat'l Sec. Agency, NSA Stops Certain Section 702 "Upstream" Activities (Apr. 28, 2017) (here).
- Off. of the Dir. of Nat'l Intel., The FISA Amendments Act: Q&A (Unclassified) (April 18, 2017) (here).
- Joint Statement of Bradley Brooker, Off. of the Dir. of Nat'l Intel., Stuart J. Evans, Dept. of Just., Grant Mendenhall, Fed. Bureau of Investigation, Paul Morris, Nat'l Sec. Agency, & Stephen Vanech, Nat'l Sec. Agency, before the Judiciary Comm., U.S. House of Representatives, Hearing: "Section 702 of the FISA Amendments Act" (Mar. 1, 2017) (here).

Continued on next page

Appendix A: The following publicly available sources were reviewed and analyzed to produce the Section 702 Assessment. (cont.)

- Nat'l Counterterrorism Ctr., NCTC Foreign Intelligence Surveillance Act Section 702 (2017) (here).
- Letter from Robert S. Litt, Off. of the Dir. of Nat'l Intel., to Justin S. Antonipillai, Dept. of Comm. & Ted Dean, Int'l Trade Admin. (Feb. 22, 2016) (here).
- Priv. and C.L. Oversight Bd., Recommendations Assessment Report (Feb. 5, 2016) (here).
- Priv. and C.L. Oversight Bd., Recommendations Assessment Report (Jan. 29, 2015) (here).
- Priv. and C.L. Oversight Bd., Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (July 2, 2014) (here).
- Nat'l Sec. Agency Dir. Of C.L. and Priv. Off., NSA's Implementation of Foreign Intelligence Surveillance Act Section 702 (Apr. 16, 2014) (here).
- Off. of the Dir. of Nat'l Intel., Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (June 8, 2013) (here).
- Richard A. Clarke et al., Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies (Dec. 12, 2013) (here).
- Letter from Kathleen Turner, Off. of the Dir. of Nat'l Intel. & Ronald Weich, Dept. of Just. to Mike Rogers & C.A. Dutch Ruppersberger, Permanent Select Comm. on Intel., U.S. House of Representatives (May 4, 2012) (here).
- Off. of the Dir. of Nat'l Intel., The FISA Amendments Reauthorization Act of 2017: Enhanced Privacy Safeguards for Personal Data Transfers Under Privacy Shield (undated) (here).
- Off. of the Dir. of Nat'l Intel., Fact Sheet: Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (undated) (here).
- Off. of the Dir. of Nat'l Intel., Section 702 Overview (undated) (here).
- Nat'l Sec. Agency, Updated FAA 702 Targeting Review Guidance (undated) (here).
- Nat'l Sec. Agency, FAA 702 Practical Applications (undated) (here).
- Nat'l Sec. Agency, FAA 702 Adjudicator Training (undated) (here).
- Nat'l Sec. Agency, FAA Adjudication Checklist (undated) (here).

Continued on next page

Appendix A: The following publicly available sources were reviewed and analyzed to produce the Section 702 Assessment.

FISC

FISC 2019 Certification of Section 702 Surveillance Program

- [Redacted] Memorandum Opinion and Order (FISC Dec. 6, 2019) (here).
- Fed. Bureau of Investigation, Targeting Procedures (filed Sept. 17, 2019) (here).
- Nat'l Sec. Agency, Targeting Procedures (filed Sept. 17, 2019) (here).
- Cent. Intel. Agency, Minimization Procedures (filed Sept. 17, 2019) (here).
- Fed. Bureau of Investigation, Minimization Procedures (filed Sept. 17, 2019) (here).
- Nat'l Counterterrorism Ctr., Minimization Procedures (filed Sept. 17, 2019) (here).
- Nat'l Sec. Agency, Minimization Procedures (filed Sept. 17, 2019) (here).
- Cent. Intel. Agency, Querying Procedures (filed Sept. 17, 2019) (here).
- Fed. Bureau of Investigation, Querying Procedures (filed Sept. 17, 2019) (here).
- Nat'l Counterterrorism Ctr., Querying Procedures (filed Sept. 17, 2019) (here).
- Nat'l Sec. Agency, Querying Procedures (filed Sept. 17, 2019) (here).

FISC 2018 Certification of Section 702 Surveillance Program

- [Redacted] Memorandum Opinion and Order (FISC Sept. 4, 2019) (here).
- In re: DNI/AG Certifications 2018 [Redacted] (FISCR July 12, 2019) (here).
- [Redacted] Memorandum Opinion and Order (FISC Oct. 18, 2018) (here).
- [Redacted] Order (FISC Apr. 5, 2018) (here).
- Fed. Bureau of Investigation, Targeting Procedures (filed Mar. 27, 2018) (here).
- Nat'l Sec. Agency, Targeting Procedures (filed Mar. 27, 2018) (here).
- Cent. Intel. Agency, Minimization Procedures (filed Mar. 27, 2018) (here).
- Fed. Bureau of Investigation, Minimization Procedures (filed Mar. 27, 2018) (here).
- Nat'l Counterterrorism Ctr., Minimization Procedures (filed Mar. 27, 2018) (here).
- Nat'l Sec. Agency, Minimization Procedures (filed Mar. 27, 2018) (here).
- Consolidated Querying Procedures (filed March 27, 2018) (here).
- Cent. Intel. Agency, Amended Minimization Procedures (filed Sept. 18, 2018) (here).
- Fed. Bureau of Investigation, Amended Minimization Procedures (filed Sept. 18, 2018) (here).

Continued on next page

Appendix A: The following publicly available sources were reviewed and analyzed to produce the Section 702 Assessment. (cont.)

- Nat'l Counterterrorism Ctr., Amended Minimization Procedures (filed Sept. 18, 2018) (here).
- Nat'l Sec. Agency, Amended Minimization Procedures (filed Sept. 18, 2018) (here).
- Cent. Intel. Agency, Querying Procedures (filed Sept. 18, 2018) (here).
- Fed. Bureau of Investigation, Querying Procedures (filed Sept. 18, 2018) (here).
- Nat'l Counterterrorism Ctr., Querying Procedures (filed Sept. 18, 2018) (here).
- Nat'l Sec. Agency, Querying Procedures (filed Sept. 18, 2018) (here).
- Fed. Bureau of Investigation, Amended Querying Procedures (filed Aug. 12, 2019) (here).
- FISC 2016 Certification of Section 702 Surveillance Program
- [Redacted] Order (FISC Oct. 26, 2016) (here).
- [Redacted] Memorandum Opinion and Order (FISC April 26, 2017) (here).
- Nat'l Sec. Agency, Amended Minimization Procedures (filed Mar. 30, 2017) (here).
- Nat'l Sec. Agency, Amended Targeting Procedures (filed Mar. 30, 2017) (here).
- Cent. Intel. Agency, Minimization Procedures (filed Sept. 26, 2016) (here).
- Fed. Bureau of Investigation, Minimization Procedures (filed Sept. 26, 2016) (here).
- Nat'l Counterterrorism Ctr., Minimization Procedures (filed Sept. 26, 2016) (here).
- Fed. Bureau of Investigation, Targeting Procedures (filed Sept. 26, 2016) (here).
- Affidavit of James B. Comey, Dir., Fed. Bureau of Investigation (filed Sept. 26, 2016) (here).
- Affidavit of the Dir., Cent. Intel. Agency (filed Sept. 26, 2016) (here).
- Affidavit of the Dir., Nat'l Counterterrorism Ctr. (filed Sept. 26, 2016) (here).

Other Courts

- Wikimedia Found. v. Nat'l Sec. Agency/Cent. Sec. Serv., 427 F.Supp.3d 582 (D. Md. Dec. 16, 2019).
- United States v. Hasbajrami, 945 F.3d 641 (2d Cir. 2019).
- Wikimedia Found. v. Nat'l Sec. Agency, 335 F. Supp. 3d 772 (D. Md. Aug. 10, 2018).
- Klayman v. Nat'l Sec. Agency, 280 F. Supp. 3d 39 (D.D.C. Nov. 21, 2017).
- Wikimedia Found. v. Nat'l Sec. Agency, 857 F.3d 193 (4th Cir. 2017).
- Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013).

Appendix
Annex 2

Annex 2: Organizational supplementary protective measures implemented for Microsoft online services

Data importer provides the additional safeguards as described in Appendix C - Additional Safeguard Addendum to the DPA for data transferred to it as the data importer.

Data importer will implement and maintain appropriate technical and organizational measures to protect Customer Data, Professional Services Data, and Personal Data against accidental 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. Data importer 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 Customer.

Domain	Practices
Organization of Information Security ------	**Security Ownership.** Data importer has appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures. **Security Roles and Responsibilities.** Data importer personnel with access to Customer Data, Personal Data or Professional Services Data are subject to confidentiality obligations. **Risk Management Program.** Data importer performed a risk assessment before processing the Customer Data, Personal Data or Professional Services Data or launching the Online Services or Professional Services. Data importer retains its security documents pursuant to its retention requirements after they are no longer in effect.
Asset Management ------	**Asset Inventory.** Data importer maintains an inventory of all media on which Customer Data, Personal Data or Professional Services Data is stored. Access to the inventories of such media is restricted to the data importer personnel authorized in writing to have such access.

Continued on next page

Annex 2: Organizational supplementary protective measures implemented for Microsoft online services (cont.)

Domain	Practices
Asset Management (cont.) ---	**Asset Handling.** • Data importer classifies Customer Data, Personal Data or Professional Services Data to help identify it and to allow for access to it to be appropriately restricted. • Data importer has procedures for disposing of printed materials that contain Customer Data, Personal Data or Professional Services Data. • Data importer personnel must obtain data importer's authorization prior to storing Customer Data, Personal Data or Professional Services Data on portable devices, remotely accessing such data, or processing such data outside the data importer's facilities.
Human Resources Security ---	**Security Training.** Data importer informs its personnel about relevant security procedures and their respective roles. Data importer also informs its personnel of possible consequences of breaching the security rules and procedures.
Physical and Environmental Security ---	**Physical Access to Facilities.** Data importer limits access to facilities where information systems that process Customer Data, Personal Data or Professional Services Data are located to identified authorized individuals. **Physical Access to Components.** Data importer maintains records of the incoming and outgoing media containing Customer Data, Personal 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.** Data importer uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference.

Continued on next page

Annex 2: Organizational supplementary protective measures implemented for Microsoft online services (cont.)

Domain	Practices
Physical and Environmental Security (cont.) ------	**Component Disposal.** Data importer uses industry standard processes to delete Customer Data, Personal Data or Professional Services Data when it is no longer needed. **Physical Access to Components.** Data importer maintains records of the incoming and outgoing media containing Customer Data, Personal 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.** Data importer uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference. **Component Disposal.** Data importer uses industry standard processes to delete Customer Data, Personal Data or Professional Services Data when it is no longer needed.
Communications and Operations Management ------	**Operational Policy.** Data importer maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Customer Data, Personal Data or Professional Services Data. **Data Recovery Procedures.** • On an ongoing basis, but in no case less frequently than once a week (unless no Customer Data, Personal Data or Professional Services Data has been updated during that period), the data importer maintains multiple copies of Customer Data, Personal Data or Professional Services Data from which such data can be recovered. • Data importer stores copies of Customer Data, Personal Data or Professional Services Data and data recovery procedures in a different place from where the primary computer equipment processing the Customer Data, Personal Data or Professional Services Data are located.

Continued on next page

Annex 2: Organizational supplementary protective measures implemented for Microsoft online services (cont.)

Domain	Practices
Communications and Operations Management (cont.) ------	• Data importer has specific procedures in place governing access to copies of Customer Data, Personal Data or Professional Services Data. • Data importer reviews data recovery procedures at least every twelve months. • Data importer 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** Data importer has anti-malware controls to help avoid malicious software gaining unauthorized access to Customer Data, Personal Data or Professional Services Data, including malicious software originating from public networks. **Data Beyond Boundaries.** • Data importer encrypts, or enables Customer to encrypt, Customer Data, Personal Data or Professional Services Data that is transmitted over public networks. • Data importer restricts access to Customer Data, Personal Data or Professional Services Data in media leaving its facilities. **Event Logging.** Data importer logs, or enables Customer to log, access and use of information systems containing Customer Data, Personal Data or Professional Services Data registering the access ID, time, authorization granted or denied, and relevant activity.

Continued on next page

Annex 2: Organizational supplementary protective measures implemented for Microsoft online services (cont.)

Domain	Practices
Access Control ------	**Access Policy.** Data importer maintains a record of security privileges of individuals having access to Customer Data, Personal Data or Professional Services Data. **Access Authorization** • Data importer maintains and updates a record of personnel authorized to access the data importer's systems that contain Customer Data, Personal Data or Professional Services Data. • Data importer deactivates authentication credentials that have not been used for a period of time not to exceed six months. • Data importer identifies those personnel who may grant, alter or cancel authorized access to data and resources. • Data importer ensures that where more than one individual has access to systems containing Customer Data, Personal 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, Personal Data or Professional Services Data when needed. • Data importer restricts access to Customer Data, Personal Data or Professional Services Data to only those individuals who require such access to perform their job function. **Integrity and Confidentiality.** Data importer instructs Microsoft personnel to disable administrative sessions when leaving premises the data importer controls or when computers are otherwise left unattended. Data importer stores passwords in a way that makes them unintelligible while they are in force.

Continued on next page

Annex 2: Organizational supplementary protective measures implemented for Microsoft online services (cont.)

Domain	Practices
Access Control ------	**Authentication** • Data importer uses industry standard practices to identify and authenticate users who attempt to access information systems. • Where authentication mechanisms are based on passwords, the data importer requires that the passwords are renewed regularly or uses other Multi-Factor Authentication (MFA) methods. • Where authentication mechanisms are based on passwords, the data importer requires the password to be at least eight characters long. • Data importer ensures that de-activated or expired identifiers are not granted to other individuals. • Data importer monitors, or enables Customer to monitor, repeated attempts to gain access to the information system using an invalid password. • Data importer maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed. • Data importer 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. **Network Design.** Data importer has controls to avoid individuals assuming access rights they have not been assigned to gain access to Customer Data, Personal Data or Professional Services Data they are not authorized to access.

Annex 2: Organizational supplementary protective measures implemented for Microsoft online services (cont.)

Domain	Practices
Information Security Incident Management ------	**Incident Response Process** • Data importer 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 the data importer (as described in the "Security Incident Notification" section above) will be made without undue delay and, in any event, within 72 hours. • Data importer 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.** Data importer security personnel verify logs at least every six months to propose remediation efforts if necessary.
Domain	**Practices**
Business Continuity Management ------	• Data importer maintains emergency and contingency plans for the facilities in which the data importer's information systems that process Customer Data, Personal Data or Professional Services Data are located. • Data importer's redundant storage and its procedures for recovering data are designed to attempt to reconstruct Customer Data, Personal Data or Professional Services Data in its original or last-replicated state from before the time it was lost or destroyed.

Compliance with EU transfer requirements for personal data in the Microsoft cloud

This paper provides guidance to customers of Microsoft Online Services and Professional Services (as defined in the Microsoft Products and Services Data Protection Addendum) in following the six steps the European Data Protection Board (EDPB) recommends that companies take to ensure adequate protection of personal data leaving the European Union (EU).[1]

For each step, the customer will find information about what Microsoft does, including a description of specific supplementary measures, to help support compliance with EDPB recommendations.