



Changing interpretations of General Data Protection Requirements (GDPR) when data is transferred outside of EU/EEA

Schrems II and Microsoft

Ole Tom Seierstad
National Security Officer



What data transfer agreements were in question?

Prior to Schrems II: Two overlapping protections used for data transfers

EU Standard Contractual Clauses (SCCs)

Standard Contractual Clauses (SCCs) are agreements between customers (data controllers) and their online services providers (data processors).



For years, Microsoft has used SCCs to govern the transfers of customer data in connection with our core online services, as well as the transfer of professional services data delivered under the [Microsoft Professional Services Data Protection Addendum](#) (i.e., Premier/Unified Support and Microsoft Consulting Services).

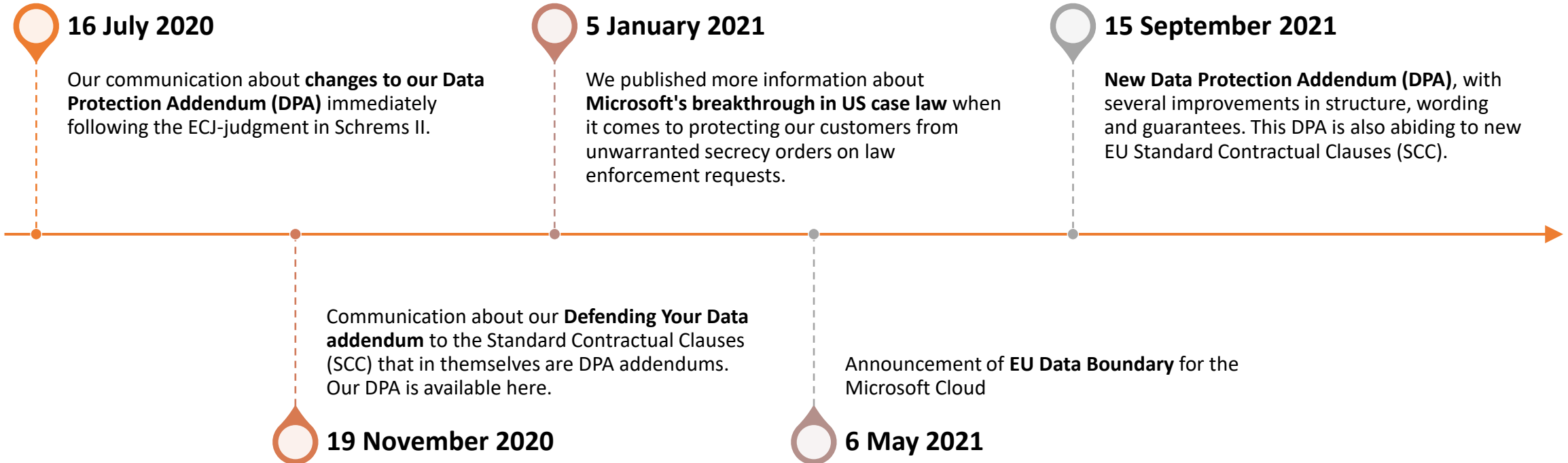
EU-US Privacy Shield

Privacy Shield was a legal framework for data transfers between the EU and US.







Microsoft has applied this framework to protect transfers of customer data from all Online Services, including some data transfers already covered by SCCs.

Timeline for Microsoft's follow-up since Schrems II



Foundational Privacy Principles

-  You control your data
-  You choose where your data is located
-  We secure your data at rest and in transit
-  We defend your data

You control your data

Our time-tested approach to privacy is grounded in our commitment to give you control over the data you put in the cloud. In other words: you control your data. Microsoft guarantees this with the contractual commitments we make to you.



Your data belongs to you

Your data is your business, and you can access, modify, or delete it at any time. Microsoft will not use your data without your agreement, and when we have your agreement, we use your data to provide only the services you have chosen.



Your control of your data

Your control over your data is reinforced by Microsoft compliance with broadly applicable privacy laws such as the GDPR and privacy standards such as the world's first international code of practice for cloud privacy, ISO/IEC 27018.

You choose where your data is located

When you use Microsoft commercial cloud services, you choose the service and data location that is right for your business.

[Learn more >](#)



Choices for datacenters

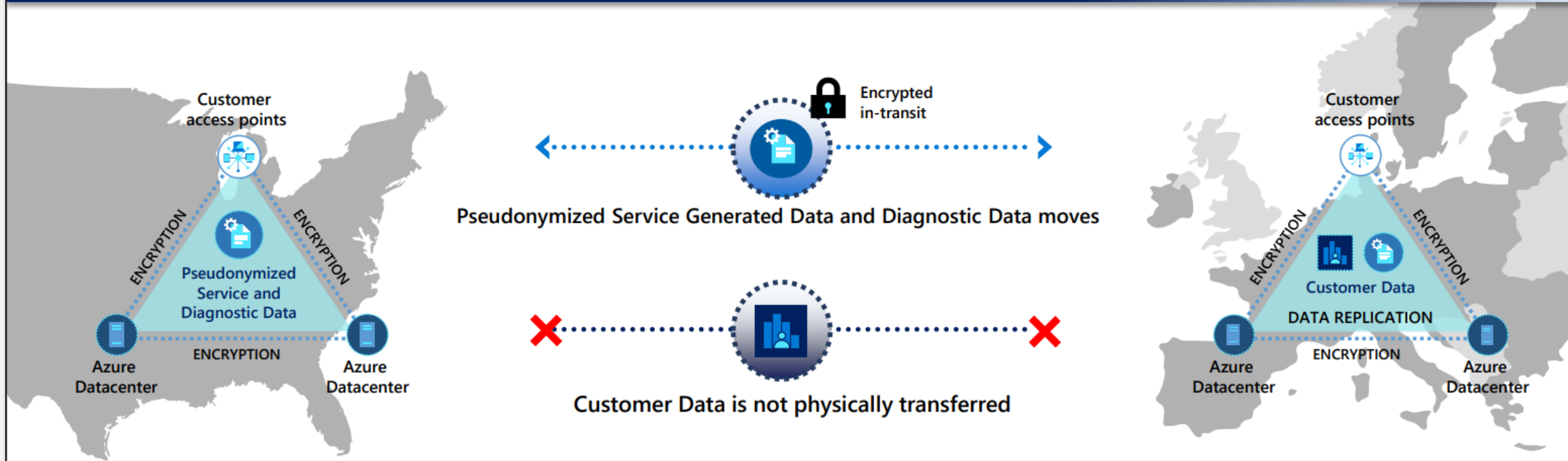
Based on your choice of Microsoft online services, we offer options and tools for determining where your data is stored when you use Microsoft Azure, Microsoft Dynamics 365 and Power Platform, and Microsoft 365 services. For example, Azure allows you to choose from more than 60 regions linked by one of the largest interconnected networks on the planet including more than 150 datacenters and growing. Microsoft 365 places new customers in the datacenter nearest your business address, with the flexibility to deploy in additional datacenters of your choice.



Choices for data residency

Because of our large and ever-expanding network of datacenters, Microsoft can offer data residency in more places in the world than any other cloud provider. This helps ensure that resiliency and compliance requirements are honored within geographic boundaries and enables customers with specific data-residency and compliance obligations to keep their data and applications close. We back these capabilities with contractual commitments to store your data within specific geographic boundaries.

Azure Regional Services – Personal Data Flow for European Union | Microsoft Initiated



Pseudonymized Service and Diagnostic Data

Usage:

- Service reliability and performance monitoring
- Fraud prevention
- Billing
- Product improvement

[More details here](#)



Customer Data

- Stored and Processed in Customer selected Geography
- Encrypted at rest and in-transit
- No access by Microsoft Personnel without Customer authorization, except in exceptional circumstances as defined [here](#)

* For data flow exceptions, see [here](#)

We secure your data at rest and in transit

With state-of-the-art encryption, Microsoft protects your data both at rest and in transit. Our encryption protocols erect barriers against unauthorized access to the data, including two or more independent encryption layers to protect against compromises of any one layer.



Data at rest

The Microsoft cloud employs a wide range of encryption capabilities up to AES-256, giving you the flexibility to choose the solution that's best for your business.



Data in transit

Data moving between user devices and Microsoft datacenters or within and between the datacenters themselves—Microsoft uses and enables the use of industry-standard encrypted transport protocols, such as Transport Layer Security (TLS) and Internet Protocol Security (IPsec).



Encryption keys

All Microsoft-managed encryption keys are properly secured and offer the use of technologies such as Azure Key Vault to help you control access to passwords, encryption keys, and other secrets.

We defend your data

Through clearly defined and well-established response policies and processes, strong contractual commitments, and if need be, the courts, Microsoft defends your data. We believe that all government requests for your data should be directed to you. We do not give any government direct or unfettered access to customer data. Microsoft is principled and transparent about how we respond to requests for data.



Responding to data requests

Because we believe that you should have control over your own data, we will not disclose data to a government or law enforcement agency, except as you direct or where required by law. Microsoft scrutinizes all government demands to ensure they are legally valid and appropriate.



Law enforcement requests

If Microsoft receives a demand for a customer's data, we will direct the requesting party to seek the data directly from the customer. If compelled to disclose or give access to any customer's data, Microsoft will promptly notify the customer and provide a copy of the demand unless legally prohibited from doing so.

New EU Standard Contractual Clauses (SCC)

- **June 4, 2021** - the European Commission issued **new SCCs** for companies to transfer personal data from the EU to non-EU **countries that do not provide “adequate” data protection** as required under EU law.
- According to the *Schrems II* decision and recommendations from the European Data Protection Board (EDPB), **the SCCs remain a valid transfer mechanism so long as they include effective mechanisms to provide an essentially equivalent level of protection** in the third country to that guaranteed within the EU.
- Microsoft views its commitments under the SCCs, in conjunction with the safeguards Microsoft provides with existing supplementary measures, including the Defending your Data protections, as helping ensure **an adequate level of data protection**.

New EDPB Recommendations as of June 21st, 2021

Step one advises exporters to map and **know their transfers**, and ensure data transferred is “adequate, relevant and limited to what is necessary” for the purposes for which it is being transferred.

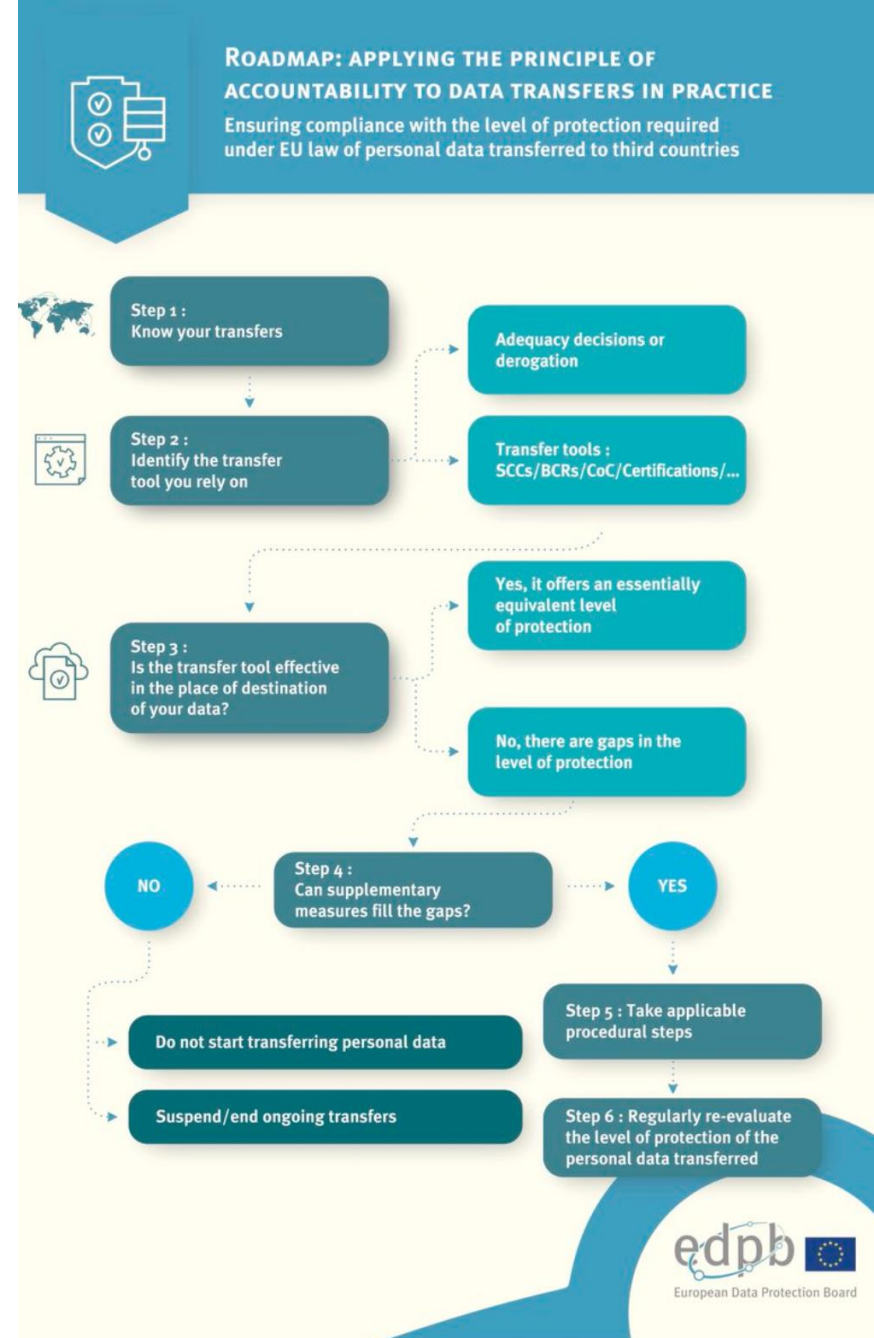
Step two is to **verify the transfer tool** the transfer relies on.

Step three is to **identify any laws or practices** of the third country

Step four. If the assessment reveals that the third country legislation impinges on the effectiveness of the Article 46 GDPR transfer tool relied upon for the transfer, step four is to **identify and adopt supplementary measures** to bring the level of data protection up to the EU standard of ‘essential equivalence’.

Step five is to **take necessary formal procedural steps** that the adoption of the chosen supplementary measure may require.

Step six is to **re-evaluate** the protected of the transferred data **at appropriate intervals** and any developments that may affect it.






EU Data Boundary for the Microsoft Cloud

Answering Europe's Call: Storing and Processing EU Data in the EU

May 6, 2021 | [Brad Smith - President and Chief Legal Officer](#)



Today we are announcing a new pledge for the European Union. If you are a commercial or public sector customer in the EU, we will go beyond our existing data storage commitments and enable you to process and store all your data in the EU. In other words, we will not need to move your data outside the EU. This commitment will apply across all of Microsoft's core cloud services – Azure, Microsoft 365, and Dynamics 365. We are beginning work immediately on this added step, and we will complete by the end of next year the implementation of all engineering work needed to execute on it. We're calling this plan the EU Data Boundary for the Microsoft Cloud.



What's this EU Data Boundary?

Data storage and processing:

- For all commercial customers located in our new EU data boundary, Microsoft will store and process the customers' personal data in the EU data boundary by the end of 2022, including diagnostic data, service-generated data, and the data Microsoft uses to provide technical support
- This strengthens and extends our current commitments around data in transit and at rest.
- This commitment will apply to Azure, Microsoft 365 (including Teams and OneDrive for Business) and Dynamics 365, as well as associated customer support operations.
- There may be a small number of instances where a particular additional feature still require the transfer of data outside the EU data boundary. We will provide customers choices over whether to enable those features.

Law Enforcement Requests and National Security Orders

Does it even matter where data is stored and
where cloud services are provided?

Defending Your Data

Microsoft was the first company to respond to the European Data Protection Board's draft recommendations with new commitments that demonstrate the strength of our conviction to defend our customers' data.

1. **First**, we are committing that **we will challenge every government request for public-sector or enterprise customers' data—from any government—where there is a lawful basis for doing so**. This strong commitment goes beyond the proposed recommendations of EDPB.
2. **Second**, we will provide **monetary compensation** to these **customers' users if we disclose their data in response to a government request in violation of the EU's GDPR**. This commitment also exceeds the EDPB's draft recommendations. It shows Microsoft is confident that we will protect our public sector and enterprise customers' data and not expose it to inappropriate disclosure.

New steps to defend your data

Nov 19, 2020 | [Julie Brill - Corporate Vice President for Global Privacy and Regulatory Affairs and Chief Privacy Officer](#)





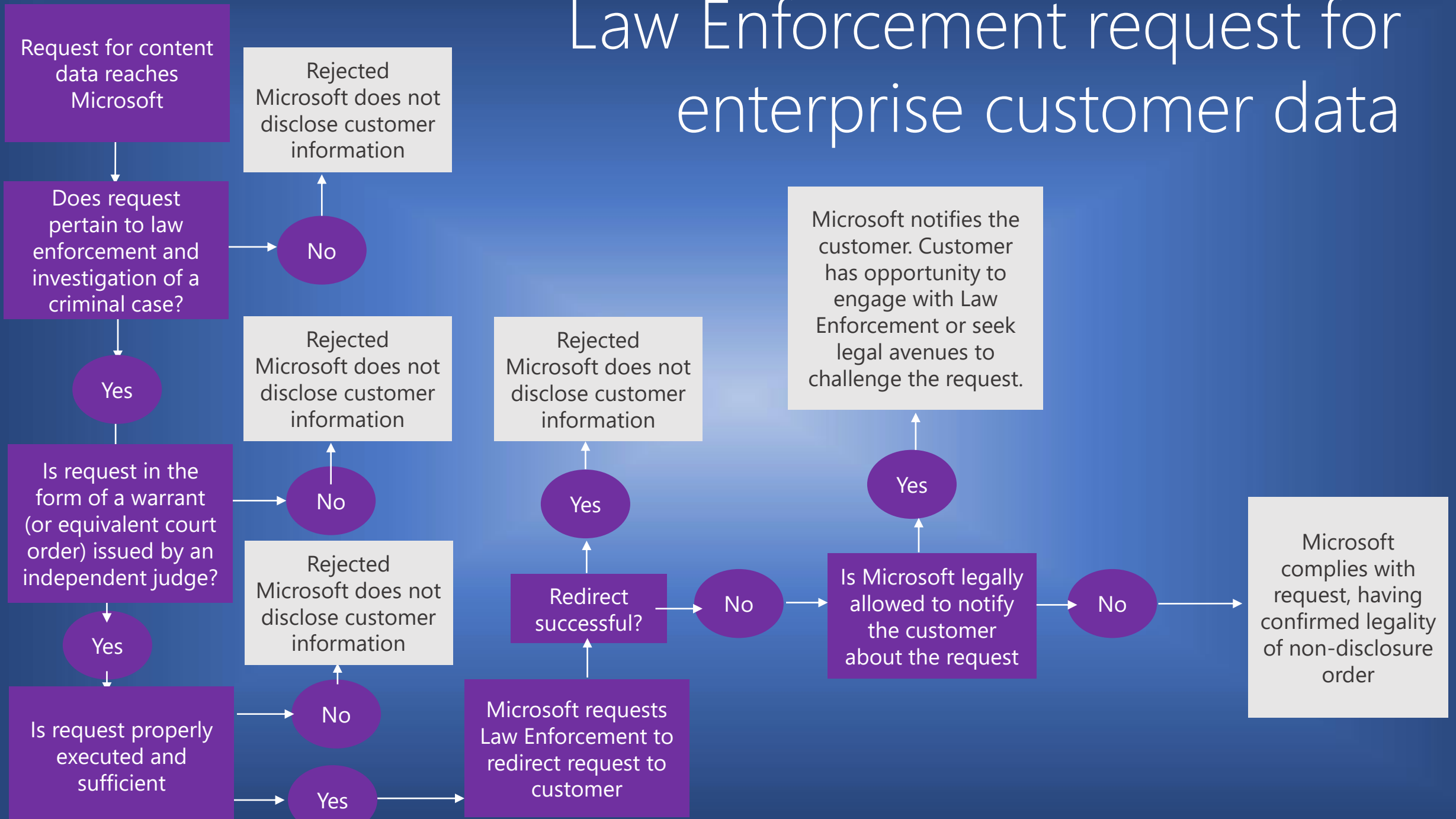
Dealing with Law Enforcement and National Security (LENS) Request

Faced with LENS-issues we rely on a set of contractual, organisational and technical measures to protect our customers' data, including [how we arrange ourselves in handling government requests for extradition of customer data](#):

1. Microsoft does not provide any government with direct and unfettered access to our customers' data, and we do not provide any government with our encryption keys or the ability to break our encryption.
2. If a government wants customer data, it must follow applicable legal process. It must serve us with a warrant or court order for content, or a subpoena for subscriber information or other noncontent data.
3. All requests must target specific accounts and identifiers.
4. Microsoft's legal compliance team reviews all requests to ensure they are valid, rejects those that are not valid, and only provides the data specified.

Our [Law Enforcement Request Report](#) and [U.S. National Security Order Report](#) are updated every six months and show that the vast majority of our customers are never impacted by government requests for data.

Law Enforcement request for enterprise customer data



Processor to Processor SCC

Available online in Microsoft Trust Center

Data Transfer Agreement (P2P)

between

Microsoft Ireland Operations Limited

hereinafter “data exporter”

and

Microsoft Corporation

hereinafter “data importer”

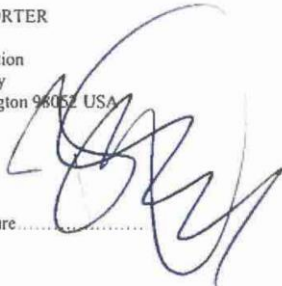
each a “party”; together “the parties”.

Dated 13 September 2021

FOR DATA IMPORTER

Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052 USA

Authorized Signature.....



FOR DATA EXPORTER

Microsoft Ireland Operations Limited
One Microsoft Place
South County Business Park
Leopardstown, Dublin 18
D18 P521, Ireland

Authorized Signature.....



Additional resources

Detailed Comparison Table

MICROSOFT PRODUCTS AND SERVICES DATA PROTECTION ADDENDUM: DETAILED COMPARISON TABLE

Dated: September 2021

MICROSOFT CONFIDENTIAL (SEPTEMBER 2021)

DPA for Products and Services	Comments/Questions
<p>The terms below are terms from the Microsoft Products & Services Data Protection Addendum, dated September 15, 2021 (the September DPA). Changes are marked against the Microsoft Online Services Data Protection Addendum, dated December 7, 2020 (the December DPA).</p>	<p>The information in this column is written to explain the changes in the September DPA. The audience is assumed to be (1) familiar with the December DPA and (2) already have some context for the changes.</p> <p>For more information on earlier versions of the DPA, please refer to announcements from those changes and prior detailed comparison tables.</p>
<p>Introduction</p> <p>The parties agree that this Microsoft Online Products and Services Data Protection Addendum ("DPA") sets forth their obligations with respect to the processing and security of Customer Data, Professional Services Data, and Personal Data in connection with the Online Products and Services. The DPA is incorporated by reference into the Online Services Product Terms (or successor location in the Use Rights and other Microsoft agreements). The parties also agree that, unless a separate Professional Services agreement exists, this DPA governs the processing and security of Professional Services Data. Separate terms, including different privacy and security terms, govern Customer's use of Non-Microsoft Products.</p> <p>In the event of any conflict or inconsistency between the DPA Terms and any other terms in Customer's volume licensing agreements, the DPA Terms shall prevail. The provisions of the DPA Terms supersede any conflicting provisions of the Microsoft Privacy Statement that otherwise may apply to processing of Customer Data, Personal Data, or Professional Services Data, as Personal Data, as defined herein. For clarity, consistent with Clause 10 of the 2020 Standard Contractual Clauses in Attachment 21, when the 2020 Standard Contractual Clauses are applicable, the 2020 Standard Contractual Clauses prevail over any other term of the DPA Terms.</p> <p>Microsoft makes the commitments in this DPA to all customers with volume license agreements. These commitments are binding on Microsoft with regard to Customer regardless of (1) the Use Rights Product Terms that may otherwise be applicable to any given Online Services Product subscription or license, or (2) any other agreement that references the Online Product Terms.</p>	<p>The major changes in the September DPA related to the following topics touched upon in the Introduction.</p> <p>Updated Standard Contractual Clauses. Microsoft updated the DPA in light of the update to the Standard Contractual Clauses.</p> <p>Integrated Terms for Products and Services. Based on customer feedback, Microsoft integrated the data protection and security terms for the commercial business. As explained in more detail below, Microsoft updated the terms that have applied to "Online Services" to apply to "Product and Services." This update allows Customers to review a single, integrated set of terms for data protection and security for Products, both Online Services and Software, and Professional Services.</p> <p>Extending the benefits of Microsoft's commitments to all customers. As was the case with the previous updates to the DPA, Microsoft extended the new terms in the September 2021 update to all commercial customers – public sector and private sector, large enterprises and small and medium businesses – globally. Microsoft's commitments apply without the requirement for an amendment or for customers to wait until the renewal of existing subscriptions or agreement. The changes are binding on Microsoft on September 15, 2021, when the updated terms were published. They will also apply to all new contracts and at the time of subscription renewal for current customers, without any additional action by customers and subject to the terms of the customer's volume license agreement.</p> <p>Online Presentation of Product Terms. Microsoft has moved to an online version of the Product Terms that will make it easier to find, print, and compare the terms in the</p>

1

Guide to DPA

MICROSOFT PRODUCTS AND SERVICES DATA PROTECTION ADDENDUM: FREQUENTLY ASKED QUESTIONS

Dated: September 2021

MICROSOFT CONFIDENTIAL (SEPTEMBER 2021)

This document provides information about the [Microsoft Products and Services Data Protection Addendum](#), published on September 15, 2021 (DPA). The changes to the DPA include:

- Microsoft's implementation of updated Standard Contractual Clauses (SCCs);
- Updates to the DPA to address customer feedback on ways Microsoft can make the data protection and security commitments clearer across Online Services, Software, and Professional Services by:
 - Integrating terms for Professional Services into the DPA;
 - More directly addressing how the DPA applies to Software, to the extent Microsoft is a processor of any personal data; and
 - Updating and simplifying definitions and language for clarity and ease of understanding.
- Continuous improvement, as part of Microsoft's regular review of DPA terms, including:
 - Expanding the scope of the Defending Your Data protections to apply to all personal data subject to GDPR, including data not transferred;
 - Adding language to reinforce Microsoft's commitment to data minimization; and
 - Strengthening the commitments for some Professional Services to align with commitments made for Core Online Services.

This document does not modify or constitute a part of your volume license agreement result from this information is subject to negotiation and execution of a definite Microsoft or, if applicable, customer's chosen authorized Microsoft reseller into commercial terms. Microsoft assumes no liability arising from your use of the MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN OR RELATING TO

This document applies to Products and Professional Services provided under the DPA and uses defined terms from the DPA and associated commercial agreements. In addition, the DPA can be used as a replacement to the previously separate [Microsoft Professional Services Data Protection Addendum](#) (the "MPSDPA"), for Customers that use Professional Services provided under the this document.

For ease of reference, this document structured as follows:

Part 1: Overview and FAQ related to the updated SCCs

Part 2: Overview and FAQ related to the integration and clarification of the DPA Appendix: Defending Your Data Protections

Additional Resources

You can report your privacy question or concern or contact Microsoft's Data Protection Officer by visiting our Privacy reporting site: <https://www.microsoft.com/en-us/concern/privacy>.

You can visit the [Microsoft Trust Center](#) for more information on our commitment to GDPR.

For easy reference, here are other resources:

- [Press release from the EDPB: EDPB adopts recommendations on supplementary measures following Schrems II](#)
- [Recommendations from the EDPB: Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data](#)
- [Implementing decision and Standard Contractual Clauses from the EC: Commission Implementing Decision \(EU\) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries](#)
- [18 November 2019 blog article](#) "Introducing more privacy transparency for our commercial cloud customers"

2



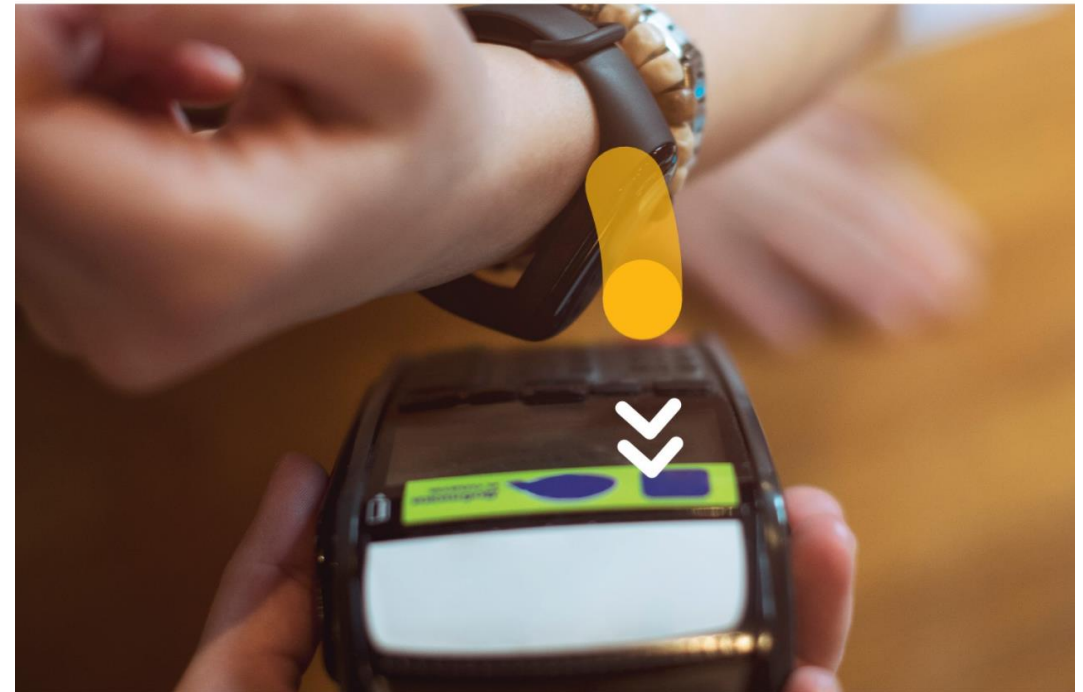
White Paper on Compliance with EU requirements

October 2021



Compliance with EU transfer requirements

for personal data in the Microsoft cloud



A glowing green padlock is centered on a blue circuit board background. The padlock is illuminated with a bright green light, making it stand out against the darker blue background. The circuit board features intricate patterns of lines and dots, suggesting a complex network or data flow. The text "Thank You!" is overlaid in white, bold, sans-serif font, positioned directly in front of the padlock.

Thank You!

Resources

New DPA

Makes Microsoft's privacy and security commitments clearer across Online Services, Software, and Professional Services by:

Integrating terms for Professional Services

More directly addressing how the DPA applies to Software Products to the extent Microsoft is a processor of any personal data

Updating and simplifying definitions and language for clarity and ease of understanding



Expanding the scope of the Defending Your Data protections to apply to all personal data subject to GDPR, including data not transferred

Adding language to reinforce Microsoft's commitment to data minimization

Strengthening the commitments for some Professional Services to align with commitments made with Core Online Services



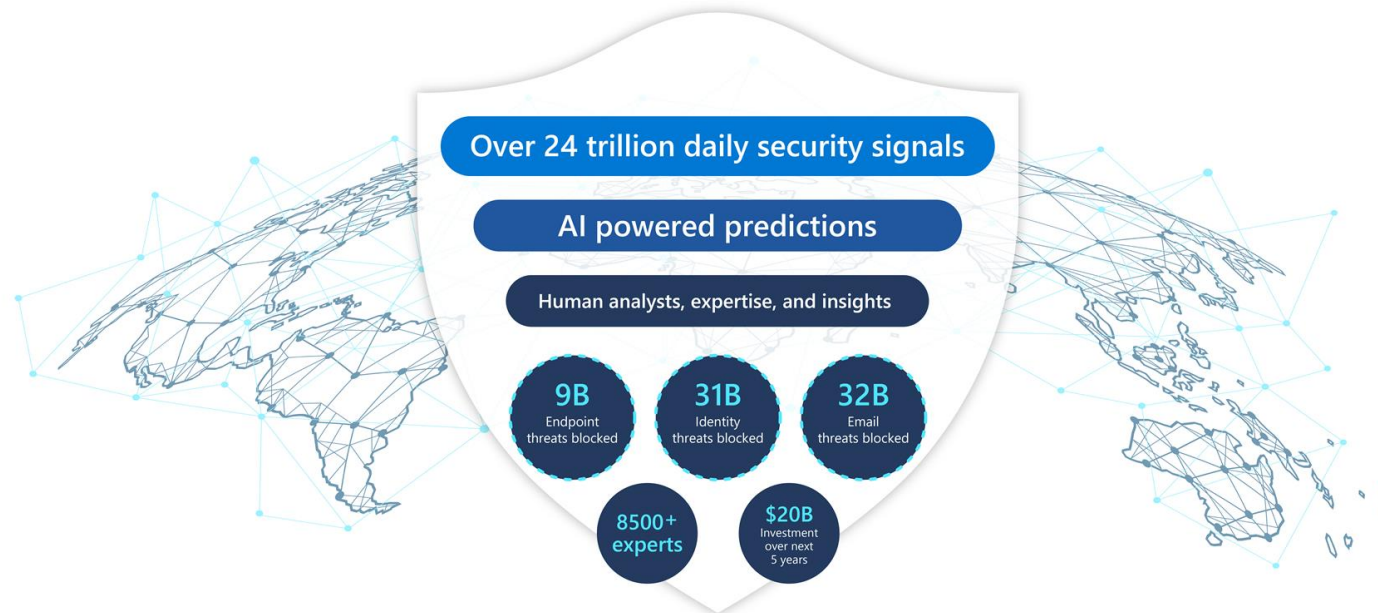
Microsoft's implementation of updated Standard Contractual Clauses (SCCs)

Doing it double right

Privacy and Security must go hand in hand

Microsoft security signals

Volume and diversity of signals processed by Microsoft



July 1, 2020 through June 30, 2021

Glossary and links to documentation



Azure Compliance Audit Reports

"Azure possess a number of important security and privacy certifications, including audit reports for ISO 27001 & 27701, ENS, HDS, FedRAMP, and NIST 800-53. These are accessible in the Azure portal [here](#).



Azure Key Vault

Azure Key Vault is a cloud service for securely storing and accessing secrets. A secret is anything that you want to tightly control access to, such as API keys, passwords, certificates, or cryptographic keys. Key Vault service supports two types of containers: Vaults and managed HSM pools. Vaults support storing software and HSM-backed keys, secrets, and certificates. [More detail here](#).



Customer Data

"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. [More detail here](#).



Customer Lockbox

Customer Lockbox for Microsoft Azure provides an interface for customers to review and approve or reject Customer Data access requests. It is used in cases where a Microsoft engineer needs to access Customer Data. [More detail here](#).



Customer Managed Key

Protection of the cryptographic keys used to protect data at rest and in transit is critical. Customer managed keys (CMK) provides the customer complete control of the key encryption key which protects the encryption at rest in their own Key Vault. Data storage services in Azure support encryption of data at rest via CMK. [More detail here](#).



Data Destruction

"When customers delete data or leave Azure, Microsoft follows strict standards for overwriting storage resources before their reuse, as well as the physical destruction of decommissioned hardware. [More detail here](#).



Diagnostic Data

"Diagnostic Data" means data collected or obtained by Microsoft from software that is locally installed by Customer in connection with the Online Service. Diagnostic Data may also be referred to as telemetry. Diagnostic Data does not include Customer Data, Service Generated Data, or Professional Services Data. [More detail here](#).



Double encryption

Double encryption is where two or more independent layers of encryption are enabled to protect against compromises of any one layer of encryption. Using two layers of encryption mitigates threats that come with encrypting data. Azure provides double encryption for data at rest and data in transit. [More detail here](#).



Encryption

Encryption is the process of encoding information which converts the original representation of the information, known as plaintext, into an alternative form known as ciphertext. Azure supports various encryption models, including server-side encryption that uses service-managed keys, customer-managed keys in Key Vault, or customer-managed keys on customer-controlled hardware. [More detail here](#).



FIPS 140.2 Standards

The Federal Information Processing Standard Publication 140-2 is a U.S. government computer security standard used to approve cryptographic modules. All Azure services use FIPS 140-2 approved algorithms for data security. Additionally, Azure customers can store their own cryptographic keys and other secrets in FIPS 140-2 validated hardware security modules (HSM). [More detail here](#).



IEEE 802.1 AE MAC Security Standards

IEEE 802.1AE (also known as MACsec) is a network security standard that operates at the medium access control layer and defines connectionless data confidentiality and integrity for media access independent protocols. Whenever Azure Customer traffic moves between datacenters-- outside physical boundaries not controlled by Microsoft (or on behalf of Microsoft)-- The packets are encrypted and decrypted on the devices before being sent, preventing physical "man-in-the-middle" or snooping/wiretapping attacks. [More detail here](#).

Glossary and links to documentation



Isolated Identity

Azure Active Directory instance is logically isolated using security boundaries to prevent Customer Data and identity information from comingling, thereby ensuring that users and administrators of one Azure AD cannot access or compromise data in another Azure AD instance, either maliciously or accidentally. [More detail here.](#)



Just-In-Time Access

Provides authorized personnel privileged, scoped access to production resources for a prescribed duration. Services administer access policies that grant access to their resources, and their DevOps engineers elevate using JIT to solve Live site incidents or support related issues. [More detail here.](#)



Multi factor authentication

Multi-factor authentication is a process where a user is prompted during the sign-in process for an additional form of identification, such as entering a code on their cellphone or to provide a fingerprint scan. [More detail here.](#)



Personal Data

"Personal Data" means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. [More detail here.](#)



Platform Managed Key

Protection of the cryptographic keys used to protect data at rest and in transit is critical. By default, Azure services uses platform management of keys for encryption at rest and in transit to ensure security and availability of these keys. [More detail here.](#)



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 an Online Service) or otherwise obtained or processed by or on behalf of Microsoft through an engagement with Microsoft to obtain Professional Services. Professional Services Data includes Support Data. [More detail here](#)



Pseudonymization

Pseudonymization is a data management and de-identification procedure by which personally identifiable information fields within a data record are replaced by one or more artificial identifiers, or pseudonym making the data record less identifiable while remaining suitable for data analysis and data processing. [More detail here.](#)



Role Based Access Control

Azure role-based access control (Azure RBAC) helps you manage who has access to Azure resources, what they can do with those resources, and what areas they have access to. Azure RBAC is an authorization system built on Azure Resource Manager that provides fine-grained access management of Azure resources. [More detail here.](#)



Service Generated Data

"Service Generated Data" means data generated or derived by Microsoft through the operation of an Online Service. Service Generated Data does not include Customer Data, Diagnostic Data, or Professional Services Data. [More detail here.](#)



Subprocessors

"Subprocessor" means other processors used by Microsoft to process Customer Data and Personal Data, as described in Article 28 of the GDPR. [More detail here.](#)



Transport Layer Security (TLS)

Transport Layer Security (TLS) is a cryptographic protocol designed to provide communications security over a computer network. All traffic leaving Azure datacenters is encrypted in transit, even if the traffic destination is another domain controller in the same region. TLS 1.2 is the default security protocol used. [More detail here.](#)