Microsoft data protection and security terms for products and services: Business operations

Microsoft Confidential

For informational purposes only

The information contained in this document is Microsoft “Confidential Information,” subject to confidentiality and non-disclosure obligations. You may not disclose any of this information to a third party without Microsoft’s prior written consent, except where Customers need to use the information to meet regulatory obligations.

This document should not be construed as legal advice. Microsoft makes no warranties, express or implied, by providing this information and nothing in this document constitutes an offer or modifies the terms or conditions of an existing agreement.

Summary

This paper provides background on processing for Microsoft business operations incident to providing products and services as described in the Microsoft Products and Services Data Protection Addendum (DPA). It is designed to help our customers understand Microsoft's business operations processing as they assess using Microsoft products and services. Microsoft also continues to review regulatory guidance and customer feedback in this area and looks for ways to keep improving our approach to further customer trust.

Unlike other large providers, which reserve full controller rights for business operations processing, Microsoft imposes data minimization requirements, use restrictions and data protection commitments for processing for business operations. In this white paper, we will take a closer look at each of those. Microsoft's DPA, which reflects the commitments for processing of personal data, Customer Data and Professional Services Data in connection with our products and services, specifies that Microsoft uses limited data for four business operations purposes – billing and account management; compensation such as calculating employee commissions and partner incentives; internal reporting and business modeling, such as forecasting, revenue, capacity planning, and product strategy; and financial reporting. To perform these business operations, Microsoft uses only aggregated or statistical data that does not single out any individual.

This section provides an overview of how Microsoft protects the personal data processed for these purposes and the limitations that Microsoft places on itself while performing these essential functions that any cloud service provider must perform.

This paper is organized in four parts:

A. Overview of processing in the Microsoft cloud

B. Background and overview on business operations

C. Detail and examples for each business operation

D. Legal bases for processing

A. Overview of processing in the Microsoft cloud

Providing a cloud service requires the cloud service provider to compute, transmit and store data to provide the service and outcomes the customer expects. These are all "processing" of the data regardless of the technical activity being performed. For example, using automation to understand and act on the content of a file, allowing automation to process the content of a file to check for malware and measuring a file to see how much storage it consumes are each processing of the file, but they are quite different technical operations and introduce different risks to privacy and confidentiality of the file.

When using Microsoft Online Services, customers provide several different types of records, any of which may contain a customer's personal data in different forms as follow:

- Information about the customer's users is synchronized to online services and forms a cloud-based copy of the directory the customer maintains in their own infrastructure. Some customers elect to reverse this model and make the Microsoft-maintained directory the authoritative directory, reducing the dependency on their own infrastructure.
- Information is provided to online services to be processed for the functional outcomes the customer wants.

For simplicity, in contractual and functional documents Microsoft calls all forms of the above "**Customer Data**" – *all data provided to Microsoft through the use of Online Services.*

Microsoft treats all Customer Data as personal data, simply because only the customer controls whether the data it provides contains personal data. The directory of users clearly will, but Microsoft does not examine Customer Data to determine if it does, in fact, contain personal data and, if it does, what categories of personal data the customer has provided. The customer decides what data to process for the functional outcome it wants.

Microsoft also comes into the possession of other data as online services are used as follows:

Diagnostic Data[1] may be collected from software the customer runs on premises if that software is provided as part of or in conjunction with the online service and used to obtain some or all of the online services outcomes. Diagnostic Data is collected so that Microsoft can tell the software is working as expected, up to date and operating securely.

System-Generated Logs[2], also known as **Service-Generated Data**[3], are generated as users interact with the online services. These records, logs and data are essential to cloud operations and the services customers have instructed Microsoft to provide. They constitute a factual record of the activity of the online services on the customer's behalf and as instructed by the customer's users and administrators. System-Generated Logs help Microsoft maintain quality, performance and capacity of the services.

[1] Not a defined term under the DPA; capitalized for the purposes of this document.

[2] Not a defined term under the DPA; capitalized for the purposes of this document.

[3] Not a defined term under the DPA; capitalized for the purposes of this document.

A. Continued

These records are particularly important where the activity interacts with Customer Data. Customers expect Microsoft to maintain records that form an audit trail of what is happening to their Customer Data – who is using it, changing it and storing or deleting it. Customer confidence in the fidelity and confidentiality of their Customer Data depends on this audit trail.

The above data sets (Customer Data, Diagnostic Data and System-Generated Logs) together form the required data to provide the cloud services a customer expects. There may be no applicable Diagnostic Data if a service does not involve any on-premises software, but there are always Customer Data and System-Generated Logs involved in using cloud services. Previously, the DPA addressed Diagnostic Data and Service-Generated Data specifically. The current DPA addresses commitments more broadly to Personal Data. Those commitments cover personal data in the categories described in this paper as Diagnostic Data and System-Generated Logs.

Privacy by Design

As noted above, Microsoft treats Customer Data as if it includes personal data. In the case of the user directory, the personal data nature of the Customer Data is obvious. In the case of Customer Data to be processed, the customer who is data controller must decide if personal data is needed for the outcomes the customer desires and if the processing meets all the requirements the customer is subject to in law, by agreement, under regulations and to serve the customer's business needs. While Microsoft is diligent in the design of cloud features to ensure the features work with only the data necessary, the customer is responsible for governance of personal data in Customer Data when using the cloud.

The analysis is different for System-Generated Logs. Microsoft software code generates these logs, and the technical design of the logging subsystems is entirely Microsoft's responsibility to ensure they are effective and comply with laws. This compliance includes data minimization: Microsoft designs logs to be generated and retained only as necessary to support security and efficacy of the online services. The management of access to the raw logs is governed by Microsoft, although Microsoft does make relevant logging available to the Customer's tenant administrators. To support data subject rights, Microsoft also offers functions to extract records from these logs if the customer requests records involving personal data of one of its users.

The service activities in the cloud are initiated by the customer's users (data subjects) or on their authority (for example, if they use service features to set up policies or automated routines). Necessarily, therefore, the audit trail of those activities must be able to identify the data subject; otherwise, it would be an ineffective audit trail.

A. Continued

This is why System-Generated Logs contain personal data. Nonetheless, Microsoft also must comply with the obligations of privacy by default and by design. Although logs are parsed and monitored by automated systems at scale to maintain high-quality operations, they may in specific cases be inspected by personnel at Microsoft, for example in case of specific customer support issues that require further investigation. If non-pseudonymized personal data directly attributable to an individual were to be retained in System-Generated Logs, then Microsoft personnel could potentially see the identity of customers' users.

Microsoft mitigates the risk to the privacy of data subjects by using privacy by default and by design. Microsoft operates to a design policy that system logging software must substitute identifiable personal data from Customer Data with pseudonyms or tokens. This can be done when the log record is recorded or can be done as a follow-up substitution (aka pseudonymization) process. In the latter case, for any time the log has identifiable personal data elements, the entire log must be protected as Customer Data and in particular protected from standing access by Microsoft personnel. Only after the identifiable personal data is removed from a log can Microsoft personnel be afforded access on a greater scale.

There are a variety of ways substituted tokens used to pseudonymize personal data in log records can be generated. The substituted token may be cyphertext generated by cryptographic means (e.g., a non-reversible hash) or a computed unique identifier or simply just a plain-text alphanumeric token pulled in sequence from a constantly growing table of pre-allocated pseudonymization tokens.

The crucial thing is that if pseudonym substitution is being conducted, the "additional information" that would re-identify the pseudonym (such as a cypher-key, user IDs, email addresses) must be stored apart from the pseudonymized record and not made available to personnel who work with the pseudonymized record. Accordingly, Microsoft limits access to token look-up tables as for Customer Data.

A. Continued

The following chart provides an overview of the obligations on and nature of the various logs:

System-Generated Logs of user activity in online service

Log records that hold any personal data directly attributable to an individual provided to Microsoft through use of the online services. benefit from the following protections: • No standing access for Microsoft personnel • Processed only in systems meeting the standards for Customer Data • Where access is granted, Microsoft management approval needed (rights-based access controls, Just-in-time access). Urgent access for personnel is therefore not viable • Personnel undergo background screening before access • Data location obligations that apply to Customer Data apply (depending on the online service, since obligations vary by service) • The personal data must be provided to customer when the customer instructs us to provide it in response to a data subject request. Service features support this requirement.	Log records that hold only pseudonymized personal data that is not directly attributable to an identified individual benefit from the following protections: • Access by Microsoft personnel based on role • Processed only in systems meeting standards for personal data • Operators need prompt access in the case of cloud outage, security events, capacity management. Post Hoc management review of access but not pre-emptive approval of access • Fewer data location restrictions – pending future phases, Microsoft's EU Data Boundary will be the first example of specific data location commitments for this data • The pseudonymized personal data must be provided to customer in case of a data subject request reporting instruction from customer, which requires re-establishing the connection with an identifiable individual to fulfill the customer's instruction.
This column includes: • Look up tables to resolve pseudonyms in System-generated Logs where they still contain the identifiable personal data or Customer Data in plaintext • Identity of users to resolve globally unique pseudonyms • If encryption is used to de-identify plain text to make it suitable for use as a cypher pseudonym in system generated data, then the key-secret for decryption must be handled as for Customer Data	This column is only • Service log records that contain personal data that has been pseudonymized.

B. Background and overview on business operations

Microsoft previously included business operations processing in the DPA as part of Microsoft's processing data for "purposes compatible with providing" the Online Services. In response to input from customers and regulators, Microsoft replaced the "compatible purposes" with more specific information in the DPA about Microsoft's "business operations." The DPA currently provides the following complete list of Microsoft's business operations necessary for providing the products and services as contracted for by the customer:

- billing and account management;
- compensation such as calculating employee commissions and partner incentives;
- internal reporting and business modeling, such as forecasting, revenue, capacity planning, and product strategy; and
- financial reporting.

This list of contractually permitted business operation activities under the DPA is consistent with Microsoft's data use policies established under the "compatible purposes" framework. The activities are inherent in cloud service providers' provision of IT services to public-sector and enterprise customers and are a direct consequence of providing technology services. With the updates to the DPA, Microsoft has committed to limiting these operations to the minimum necessary and providing transparency around them. This business operations language:

1) clarifies that Microsoft accepts the additional, applicable responsibilities as a data controller when Microsoft processes data for the specified administrative and operational purposes incident to providing the products and services (although Microsoft also accepts that a customer may consider that processing is subsumed under the customer's instructions to Microsoft as its processor);

2) clarifies that customers authorize Microsoft to:

   (i) process their personal data already generated in providing the services to create aggregated statistical, non-personal data from data containing pseudonymized identifiers (such as usage logs containing unique, pseudonymized identifiers) and

   (ii) calculate statistics related to Customer Data or Professional Services Data (both as defined in the DPA) for the four business operation purposes identified above,

   in each case without accessing or analyzing the content of Customer Data or Professional Services Data and limited to achieving only the enumerated purposes,

3) makes clear that, even if Microsoft is deemed a data controller for the limited activities of creating aggregated statistical, non-personal data or calculating statistics for the four business operations, Microsoft will not, and is not permitted to, process the customer's data for any other purposes whatsoever, and

B. Continued

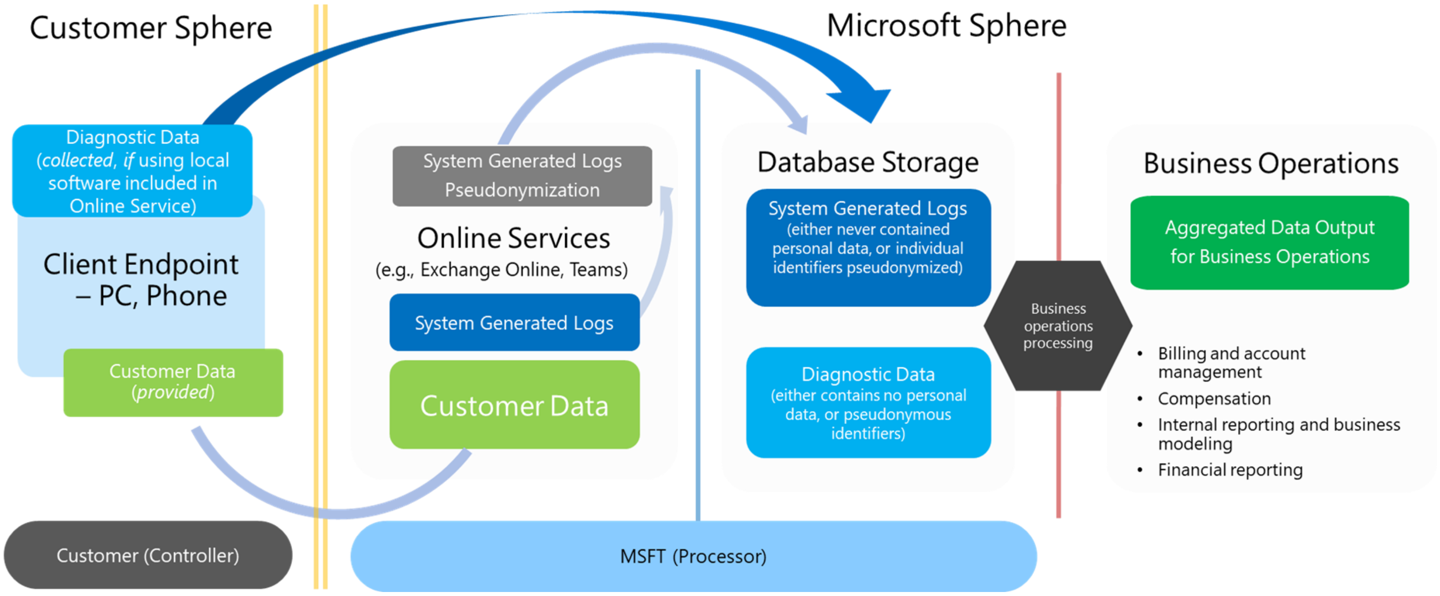
4) commits that Microsoft will not use Customer Data, Professional Services Data, or Personal Data for user profiling, advertising or similar commercial purposes. Microsoft also includes provisions that expressly address customer questions and concerns in such other areas as data minimization and the continued applicability of Microsoft's confidentiality obligations. At the same time as clarifying business operations, Microsoft also clarified the Microsoft activities that constitute "providing" the products and services to specify a clear distinction from the business operations incident to providing those products and services.

C. Details on the data used for business operations

Overview

The following graphic provides an overview of the limited personal data that serves as input for business operations processing.

Data Flows- Business Operations schematic overview


Customer Sphere
Microsoft Sphere
Diagnostic Data (*collected*, *if* using local software included in Online Service)
Client Endpoint – PC, Phone
Customer Data (*provided*)
System Generated Logs Pseudonymization
Online Services (e.g., Exchange Online, Teams)
System Generated Logs
Customer Data
Database Storage
System Generated Logs (either never contained personal data, or individual identifiers pseudonymized)
Diagnostic Data (either contains no personal data, or pseudonymous identifiers)
Business operations processing
Business Operations
Aggregated Data Output for Business Operations
Billing and account management
Compensation
Internal reporting and business modeling
Financial reporting
Customer (Controller)
MSFT (Processor)

C. Continued

As described in section A, all the data that Microsoft has as a result of providing online services is either data provided by the customer ("Customer Data," including any personal data within Customer Data) or is generated or collected by Microsoft as part of providing the services (e.g., System-Generated Logs). All of this data is obtained in Microsoft's role as a data processor. All business operations processing is performed with appropriate technical and organizational measures, as set forth in the DPA, and designed to mitigate risks to the privacy of individuals. No data containing personal data is requested, collected or generated solely for business operations purposes. Nor is any personal data transferred outside of the EU/EEA solely for business operations purposes.

Business operations processing is not applied to all Customer Data. Specifically, in no case does Microsoft permit access to or analysis of the content of Customer Data for business operations processing. Business operations "use" of Customer Data is limited to generating statistics, such as measuring the volume of Customer Data stored on servers in a data center as part of planning for required capacity expansion, without acting on what is contained within Customer Data in any cognitively relevant way. What is contained within Customer Data simply is not relevant to the business operations purposes. Indeed, business operations uses do not change Microsoft's protocols prohibiting access to Customer Data. For example, Microsoft continues to keep all access controls in place and subject to third-party audit, including zero standing access for Microsoft personnel to Customer Data content and logging all access by Microsoft personnel to Customer Data.

After the generation of statistics and aggregation of data from the input data, all business operations processing is limited to using statistics and aggregated data. The underlying input data to create the aggregation may contain pseudonymous identifiers – for example, DeviceID – generated by Microsoft in the course of providing the services to the customer, but those identifiers are not used for business operations other than for the sole purpose of creating aggregated data sets that do not themselves contain personal data. As another example of input data to create aggregations for business operations, pseudonymized identifiers in Microsoft 365 are processed alongside such previously collected data elements as platform, app, sub workload (such as Outlook or Teams or some other product), OS name/version, device type/model/manufacturer, client app/build, license type, trial/paid/free product and OEM model.

Unless deleted by the customer or by Microsoft pursuant to its retention timeframes, the underlying, unaggregated pseudonymous data remains available to the customer from Microsoft's systems that are in place to aid responding to customers' data subject requests[4]. These identifiers in the input data could be used to identify a person indirectly and are thus personal data under the GDPR, but the output that is used for business operations processing is limited to aggregated or statistical data that does not identify or single out individuals and does not contain personal data.

[4] https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-data-subject-requests

C. Continued

Nor would Microsoft want or need individual-level data for business operations purposes. Thus, for business operations purposes, Microsoft further reduces the privacy risk by aggregating the pseudonymous data so that it no longer contains any individual-level entries and has been combined with data of enough data subjects that individual-level attributes are no longer identifiable. Microsoft then relies solely on the aggregations of this pseudonymized personal data for business operations processing.

To provide an example of the flow from (1) pseudonymous personal data that is the input data to (2) aggregated data that is the output data for (3) business operations processing, the images below reflect the following:

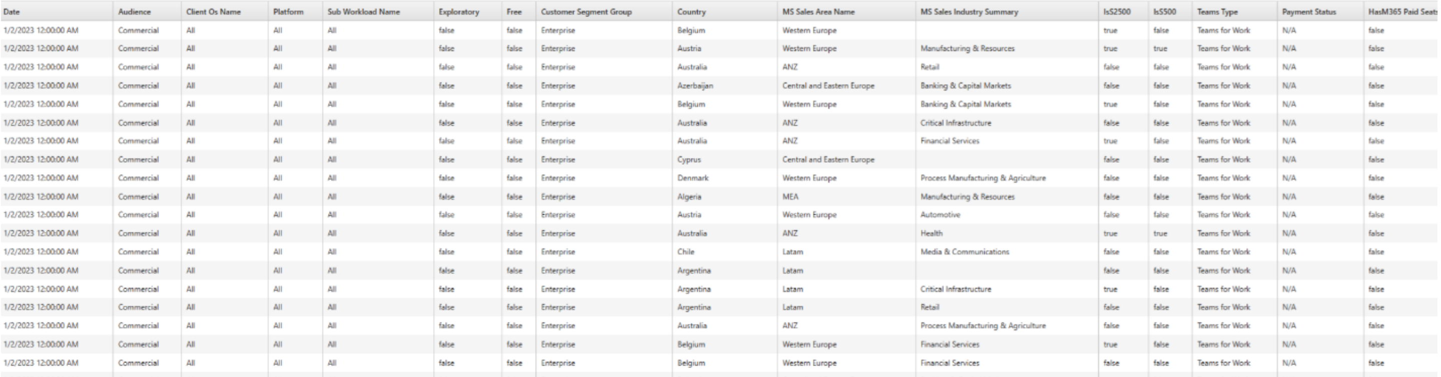
1. This shows the input of Teams Usage per tenant per user on various devices, operating systems and platforms. The associated identifier is a pseudonym:

Date	User ID	Oms Tenant ID	Audience	Application	Sub Workload Name	Usage Country Code	Platform	Client Os Name	Piblic Os Name	Device ID	Device ID Space	Device Type	Device Model	Device Manufacturer	Client Os Major Vendors	Client App Build	Client App Major Version
1/6/2023 12:00:00AM	[redacted]	[redacted]	Commercial	Teams	Other	BR	Desktop	Windows	Windows 10	[redacted]		Unknown			10	0	1
1/6/2023 12:00:00AM	[redacted]	[redacted]	Commercial	Teams	Other	BR	Desktop	Windows		[redacted]		Unknown			0		22113004100
1/6/2023 12:00:00AM	[redacted]	[redacted]	Commercial	Teams	Other	BR	Desktop	Windows		[redacted]		Unknown			0		23010505600
1/6/2023 12:00:00AM	[redacted]	[redacted]	Commercial	Teams	Other	ES	Desktop	Windows		[redacted]		Unknown	SM-F7118	Samsung	12	0	
1/6/2023 12:00:00AM	[redacted]	[redacted]	Commercial	Teams	Other	ES	Desktop	Windows	Windows 10	[redacted]		Unknown			10	0	
1/6/2023 12:00:00AM	[redacted]	[redacted]	Commercial	Teams	Other	ES	Desktop	Windows		[redacted]		Unknown			0		22113004100

▨ - This information has been redacted

C. Continued

2. This shows the output of a Count of Teams Active Usage per Country/Area/Industry:



Date	Audience	Client Os Name	Platform	Sub Workload Name	Exploratory	Free	Customer Segment Group	Country	MS Sales Area Name	MS Sales Industry Summary	IsS2500	IsS500	Teams Type	Payment Status	HasM365 Paid Seat
1/2/2023 12:00:00 AM	Commercial	All	All	All	false	false	Enterprise	Belgium	Western Europe		true	false	Teams for Work	N/A	false
1/2/2023 12:00:00 AM	Commercial	All	All	All	false	false	Enterprise	Austria	Western Europe	Manufacturing & Resources	true	true	Teams for Work	N/A	false
1/2/2023 12:00:00 AM	Commercial	All	All	All	false	false	Enterprise	Australia	ANZ	Retail	false	false	Teams for Work	N/A	false
1/2/2023 12:00:00 AM	Commercial	All	All	All	false	false	Enterprise	Azerbaijan	Central and Eastern Europe	Banking & Capital Markets	false	false	Teams for Work	N/A	false
1/2/2023 12:00:00 AM	Commercial	All	All	All	false	false	Enterprise	Belgium	Western Europe	Banking & Capital Markets	true	false	Teams for Work	N/A	false
1/2/2023 12:00:00 AM	Commercial	All	All	All	false	false	Enterprise	Australia	ANZ	Critical Infrastructure	false	false	Teams for Work	N/A	false
1/2/2023 12:00:00 AM	Commercial	All	All	All	false	false	Enterprise	Australia	ANZ	Financial Services	true	false	Teams for Work	N/A	false
1/2/2023 12:00:00 AM	Commercial	All	All	All	false	false	Enterprise	Cyprus	Central and Eastern Europe		false	false	Teams for Work	N/A	false
1/2/2023 12:00:00 AM	Commercial	All	All	All	false	false	Enterprise	Denmark	Western Europe	Process Manufacturing & Agriculture	false	false	Teams for Work	N/A	false
1/2/2023 12:00:00 AM	Commercial	All	All	All	false	false	Enterprise	Algeria	MEA	Manufacturing & Resources	false	false	Teams for Work	N/A	false
1/2/2023 12:00:00 AM	Commercial	All	All	All	false	false	Enterprise	Austria	Western Europe	Automotive	false	false	Teams for Work	N/A	false
1/2/2023 12:00:00 AM	Commercial	All	All	All	false	false	Enterprise	Australia	ANZ	Health	true	true	Teams for Work	N/A	false
1/2/2023 12:00:00 AM	Commercial	All	All	All	false	false	Enterprise	Chile	Latam	Media & Communications	false	false	Teams for Work	N/A	false
1/2/2023 12:00:00 AM	Commercial	All	All	All	false	false	Enterprise	Argentina	Latam		false	false	Teams for Work	N/A	false
1/2/2023 12:00:00 AM	Commercial	All	All	All	false	false	Enterprise	Argentina	Latam	Critical Infrastructure	true	false	Teams for Work	N/A	false
1/2/2023 12:00:00 AM	Commercial	All	All	All	false	false	Enterprise	Argentina	Latam	Retail	false	false	Teams for Work	N/A	false
1/2/2023 12:00:00 AM	Commercial	All	All	All	false	false	Enterprise	Australia	ANZ	Process Manufacturing & Agriculture	false	false	Teams for Work	N/A	false
1/2/2023 12:00:00 AM	Commercial	All	All	All	false	false	Enterprise	Belgium	Western Europe	Financial Services	true	false	Teams for Work	N/A	false
1/2/2023 12:00:00 AM	Commercial	All	All	All	false	false	Enterprise	Belgium	Western Europe	Financial Services	false	false	Teams for Work	N/A	false

3. Microsoft uses this Teams monthly active user (MAU) aggregated data for financial reporting. A variation of these aggregated MAU numbers is also used for field compensation as well as other business operations such as internal reporting to leadership.

Additional examples are in Appendix A.

C. Continued

Details on each of the four business operations

Following is a more detailed description of the processing done in connection with each of the business operations activities.

1. Customer Billing and Account Management:

Microsoft bills for some products and services based on customer usage. To bill accurately, Microsoft needs data generated or received while providing such products and services to the customer. For example, for online services billed “per user,” Microsoft needs to count the users in each customer tenancy. For online services billed based on “consumption,” Microsoft needs to measure billable usage by the customer.

Billing for products and services is based on statistics or aggregated data. As described above, the aggregated data used for billing is based on pseudonymous identifiers generated by Microsoft within System-Generated Logs. This gives Microsoft the information it needs to create accurate bills and work through any questions related to billing (e.g., the amount of a service level credit), while limiting the processing of Customer Data and personal data to the minimum required (consistent with data usage minimization principles that apply across all business operations).

As part of this business operations activity, Microsoft also uses aggregated data for account management for customers who engage with Microsoft personnel or partners assigned to their accounts (e.g., a technical account manager).

Microsoft manages customer accounts by assessing (and sometimes sharing with the customer) aggregated information about usage to allow Microsoft personnel (or partners managing the customers’ accounts) to have informed interactions with the customers to help them evaluate usage patterns, more effectively manage expenses and optimize future expenditures. For example, the technical or account personnel who interact with the customer need to understand aggregate information about usage of products or services by the customer to help the customer identify if there are other features that would benefit them and to obtain the greatest value from services for which they pay. Data used for account management business operations is aggregated at the level of customer organization for a given service. An exception to this is for customers that operate with multiple agreements, tenants or partners, in which case the data may be aggregated at a level based on the more complex relationship.

If the customer pays through Microsoft partners, those partners will bill the customer and perform at least some of the account management functions for the customer. In those cases, Microsoft may share the aggregated data needed to perform billing and account management with the partner providing those functions, subject to confidentiality obligations.

Consistent with its practices around all business operations, Microsoft does not permit people working on billing or account management as part of this business operation to: (a) see usage by individuals or to re-identify individuals from the pseudonymous identifiers; or (b) access the content of Customer Data, including personal data within the content of Customer Data or Professional Services Data.

C. Continued

2. Compensation:

To ensure that customers and users are activating and getting value from their purchases, Microsoft compensates both Microsoft personnel and our partners on usage-based metrics (e.g., calculating employee commissions and partner incentives based on usage of their customers). Each of the metrics used is designed to measure whether users are activating and getting value from purchased products. To calculate usage-based metrics, Microsoft needs to count users or usage at a customer level, within a service, within a customer segment, or using other aggregated measures. As explained in more detail above, those counts are based on aggregations of data containing pseudonymous identifiers generated by Microsoft within System-Generated Logs in the course of providing the service to the customers. For example, usage-based compensation may involve counting the number of users who have sent at least one email in a month or the average mailbox size. Data used to calculate compensation is aggregated at least to the level of customer organization for a given service. An exception to this is for customers that operate with multiple agreements, tenants, or partners, in which case the data may be aggregated to a level based on the more complex relationship.

As with other business operations, Microsoft does not permit people involved in calculating or receiving compensation as part of this business operations activity to: (a) see usage by individuals or to re-identify individuals from the pseudonymous identifiers; or (b) access the content of Customer Data, including personal data within the content of Customer Data or Professional Services Data.

3. Microsoft Internal Reporting and Business Modelling:

Microsoft uses aggregated data for internal reporting and business modelling for such purposes as forecasting, capacity and business planning, and product strategy. For example, if Microsoft releases a new feature, Microsoft may use aggregated, non-personal, usage data to determine whether customers are using the feature and thus getting value out of it. That, in turn, can help Microsoft invest in improving features to make them more useful. In addition, aggregated region- and market-level data enables Microsoft product teams, including Exchange, Teams and Azure, to assess usage across different regions and markets and forecast capacity needs, for example to meet the increased demand from remote work.

Microsoft’s internal reporting and modelling is based on usage data aggregated across multiple customers in most cases vs. being limited to usage data aggregated from a single customer’s tenant. Microsoft’s analysis of usage is typically across all customers or in market segments, e.g., number of users who use a given service capability, amount of usage on servers for a specific online service, or adoption of a service capability in different market segments (e.g., small business, large organizations).

Once again, Microsoft does not permit people involved in internal reporting or modelling as part of this business operations activity to: (a) see usage by individuals or to re-identify individuals from the pseudonymous identifiers; or (b) access the content of Customer Data, including personal data within the content of Customer Data or Professional Services Data.

C. Continued

4. Financial reporting:

Microsoft must comply with applicable laws and regulations, including those designed to ensure the transparency and efficient functioning of markets. In the vast majority of situations, these obligations can be satisfied through the use of aggregated data based on pseudonymous identifiers generated by Microsoft (as described in more detail above). For example, to develop the information needed to meet its financial reporting obligations, Microsoft processes pseudonymous identifiers that had been generated in the course of providing the services to customers to build aggregate information across large segments of Microsoft's customers to report on sales and usage. This includes, for example, aggregations of monthly active users of Microsoft 365. The data is used for required reporting Microsoft makes to the U.S. Securities and Exchange Commission (SEC).[5]

As with all business operations, Microsoft does not permit people involved with financial reporting as part of this business operations activity to: (a) see usage by individuals or to re-identify individuals from the pseudonymous identifiers; or (b) access the content of Customer Data, including personal data within the content of Customer Data or Professional Services Data.

[5] The financial reporting and disclosure rules in most EU Member States are broadly analogous to the U.S. SEC rules. In Germany, for example, companies listed on a German stock exchange must file annual and semi-annual reports that meet German and EU financial disclosure obligations, compliance with which is enforced by the German Federal Financial Supervisory Authority (BaFin). Similarly, in Ireland, companies listed on Euronext Dublin (formerly the Irish Stock Exchange) must comply with the Transparency (Directive 2004/109/EC) Regulations 2007 and related rules, which are enforced by the Central Bank of Ireland and Irish Auditing and Accounting Supervisory Authority. Although these Member State rules do not apply directly to Microsoft—given that Microsoft is not listed on any stock exchange in these jurisdictions—the disclosure obligations they impose on listed companies would likely be broadly in line with those imposed on Microsoft under U.S. law.

D. Legal bases for processing

Overview

Microsoft provides the following information to support our customers' assessment of the legal bases under EU data protection law for processing the four business operations identified in the DPA. Because the processing is inextricably linked to providing the customer the services they request, as noted above in Section B, previously Microsoft described this limited processing as purposes compatible with providing the services, for which we act as a processor. However, due to customer and regulatory input, we recognize some would construe this processing as operating as a controller. Thus, as applicable based on regulatory interpretation in a given jurisdiction, the processing would consist either of

(i) Microsoft taking on controller responsibilities related to generating statistics or aggregated data from pseudonymized personal data that had previously been generated or collected to provide the service and Microsoft using that aggregated data for business operations purposes, subject to Microsoft being contractually limited to aggregating the pseudonymized personal data for the four business operations, or

(ii) Microsoft performing the processing operation of generating statistics or aggregating the pseudonymized personal data as a processor on behalf of the customer and pursuant to the customer's instructions to generate statistics or aggregate data from pseudonymized personal data that had previously been generated or collected to provide the service for the four business operations.

Depending on the customer, the legal basis would be legitimate interest under GDPR Article 6(1)(f) (for most customers), public interest under GDPR Article 6(1)(e) (for public-sector customers subject to the GDPR) or public interest under Regulation (EU) 2018/1725 Article 5(1)(a) (for EU institutions that are not subject to the GDPR). It could also extend to GDPR Article 6(1)(c) or Regulation (EU) 2018/1725 Article 5(1)(c) where, depending on the customer's legal obligations, the overall purpose of the processing is needed to comply with a legal obligation of the controller (i.e., the customer).

For each of the four business operations, this paper provides examples of the processing at issue (see Section C above), explains the legitimate interest or public interest legal basis, and identifies the safeguards Microsoft puts in place that ensure the proportionality of the processing in light of those interests. Microsoft believes that there are compelling reasons to support customers' authorization or, as applicable, customers' instruction, to Microsoft to perform each of these business operations as summarised and then described more fully, below.

First, for each business operation, Microsoft (a) only uses statistical or aggregated non-personal data for achieving the business operations purposes, such data being created by cumulatively applying aggregation and pseudonymization measures to already very limited personal data or by calculating statistics about Customer Data, in both cases without accessing or analyzing the content of Customer Data or Professional Services Data and (b) deploys additional safeguards effectively blocking a reversal of such measures in business operations processing, in order to avoid prejudice to data subjects' interests and to ensure the proportionality of the data processing.

D. Continued

Second, applying GDPR Article 6(1)(f), the processing for business operations is necessary for the purposes of the legitimate interests of achieving the limited business operations purposes while – in light of the aggregated, pseudonymized and limited data of the data subjects at issue – the countervailing interests and fundamental rights and freedoms of the data subjects do not override that legitimate interest.

Third, for public-sector customers, each of the business operations is necessary for a task carried out in the public interest – both in the sense that the processing enables good management by the customers that will make use of Microsoft's products and the proper functioning of those public-sector entities and, as applicable, in the sense of advancing specific tasks imposed by law on those entities.

Analysis to assist customers

Microsoft provides the following analysis to assist customers in demonstrating application of GDPR Article 6(1)(f) and GDPR Article 6(1)(e) (or Regulation (EU) 2018/1725 Article 5(1)(a)) to business operations processing:

1) GDPR Article 6(1)(f) states that (emphasis added)

> *"Processing shall be lawful only if and to the extent that at least one of the following applies: […] (f) processing is necessary for the purposes of the legitimate interests pursued by the controller* ***or*** *by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."*,

which leads to the following three-step analysis being required:

(i) **Legitimate interest:** There have to be legitimate interests pursued by the controller (i.e., Microsoft or the customer) or a third party;

(ii) **Necessity:** The processing of the personal data must be necessary for the purpose of reaching the legitimate interests (i.e., the processing must be the mildest of all available objectively suitable means for reaching the legitimate interests);

(iii) **No overriding interests:** There must not be any overriding interests or fundamental rights and freedoms (requiring protection of personal data) of the data subject, which requires identifying the data subjects' contrary interests and weighing them against the legitimate interests.

D. Continued

Here is the three-step analysis for the business operations described above:

Processing measures: Processing for business operations			
(i) legitimate interest	**(ii) necessity**	**(iii) No overriding interests**	
		contrary interest	*weighing of interests*
There are legitimate interests of both Microsoft and the customer regarding the processing of data in the context of business operations: 1) **Microsoft’s legitimate interest** Offering modern, state-of-the-art services and achieving the business operations described above. 2) **Customer’s legitimate interest** Using the limited subset of statistical data or aggregated and pseudonymized personal data and thus being able to use state-of-the-art services.	The limited data used for business operations processing are objectively necessary to achieve the described legitimate interests. There is no milder means. While the aggregated data is non-personal and does not permit singling out individuals, it would not, for example, be possible to use anonymous data to develop the aggregations since this would not allow reaching the business operations purposes.	It could be argued that any data subject has the interest of their personal data not being processed and, where this occurs, that the processed personal data are limited to what is necessary for reaching the purposes.	The weighing of interests goes beyond juxtaposing the legitimate interests and the contrary interests. It has in particular to take into account 1) the nature of the respective interests, 2) the intensity with which the respective interests are affected by the measure being undertaken and 3) whether the data subjects have been informed in a transparent fashion and whether the controller ensures that the data subjects have a point of contact (i.e., Microsoft). With regard to the processing for business operations in the case at hand the following parameters lead to the legitimate interests outweighing the data subjects’ contrary interests: 1) The data concerned are very limited. The data used for business operations do not contain information about individual traits of data subjects. 2) The intensity with which Microsoft’s interests are affected by the processing operations not being carried out as planned would be very high for Microsoft. Microsoft would lose its ability to offer state-of-the-art services. In contrast, for the data subjects the effect of the processing for business operations being carried out as planned only has a theoretic effect, especially in light of the fact that only statistical or aggregated and pseudonymized data are processed (see above) and that the data are very limited. 3) Via disclosures in the Microsoft Privacy Statement, Microsoft has transparently informed the data subjects and offered to stay their unique point of contact as regards their privacy rights.

D. Continued

2) GDPR Article 6(1)(f) states that (emphasis added)

> *"Processing shall be lawful only if and to the extent that at least one of the following applies: [...] (e) processing is* *necessary* *for* *the performance of a task carried out in the public interest* *or in the* *exercise of official authority* *vested in the controller.",*

Similarly, Regulation (EU) 2018/1725 Article 5(1)(a) states that (emphasis added)

> *"Processing shall be lawful only if and to the extent that at least one of the following applies: [...] (a) processing is* *necessary* *for* *the performance of a task carried out in the public interest* *or in the* *exercise of official authority* *vested in the Union institution or body.",*

which leads to the following two-step analysis being required and on which governmental bodies / authorities may base the processing of the data for business operations:

(i) **Task in the public interest or exercise of official authority:** The data processing must be conducted to fulfill a task carried out in the public interest or to exercise an official authority, which requires identifying the public interest or the official authority exercised by the official authority.

(ii) **Necessity:** The processing of the personal data must be necessary for the purpose of performing a task carried out in the public interest or in exercising an official authority (i.e., the processing must be the mildest of all available objectively suitable means for reaching the public interest or exercise of official authority);

D. Continued

Here is the two-step analysis for the business operations described above:

Processing measures: Processing for business operations	
(i) Task carried out in the public interest / exercise of official authority	**(ii) necessity**
When carrying out tasks in the public interest or exercising official authority, governmental bodies / authorities are dependent on suitable tools, measures and means to do so. The use of the data for business operations processing is in this context inextricably linked with the use of the offering of Microsoft, i.e., modern, state-of-the-art services to achieve such tasks / purpose and hence using the limited subset of statistical or of aggregated and pseudonymized personal data for the business operations (as an integral part of using the respective state-of-the-art service) and thus being able to use state-of-the-art services needs to be seen as part of carrying out their tasks in the public interest / exercising their official authority (where such is facilitated by the use of such services).	The data are objectively suitable to carry out the task / exercise the official authority (by using state-of-the-art services for doing so). There are no milder means. It would for example not be possible to use anonymous data to develop the aggregations since this would not allow reaching the business operations purposes that are inextricably linked with the use of state-of-the-art services used by governmental bodies / authorities to fulfil their tasks in the public interest / exercise their official authority.

D. Continued

Details

Support for each of these business operations is described in detail below.

1. Billing and Preparing Invoices; Account Management
   a. Data Processing is Proportionate and Does Not Prejudice Rights and Freedoms of Individuals

Microsoft implements a usage-based payment model by processing a limited amount of data that Microsoft collects from online services to accurately bill the customers based on their consumption. Thus, Microsoft's bills to customers reflect actual usage by all of their relevant end users. When Microsoft processes data under this model, it uses statistical data or data containing pseudonymous identifiers that has already been collected or generated through the customers' use of the services; no additional data is collected for billing or preparing invoices. In addition, Microsoft does not re-identify individuals from the pseudonymous identifiers. Further, as noted above, Microsoft does not permit access to the content of data that a customer places into the services when processing for this purpose.

Similarly, the processing involved with account management is also proportionate and subject to safeguards to avoid risks to individuals. As with billing and preparing invoices, when Microsoft processes data for account management, it uses data containing pseudonymous identifiers that has already been collected or generated through the customers' use of the services; additional data is not collected solely for account management, and Microsoft does not re-identify individuals from the pseudonymous identifiers. And, once again, Microsoft does not permit access the content of data that a customer places into the services when processing for this purpose.

   b. Legitimate and Public Interests Bases

Customers' ability to manage their accounts and expenditures is based on the ability of Microsoft personnel and customer personnel to have meaningful and substantive discussions about the customers' IT needs and consumption. Such discussions are facilitated when Microsoft personnel can view what features of Microsoft's products customers are using and help the customers identify if there are other features that would benefit the customers. This is essential to the customers' proper account management and governance functions, and it serves the public or legitimate interest of customers for Microsoft personnel to be able to provide aggregated information about consumption and usage so that the customers can evaluate usage patterns, understand cost-efficacy, and help optimize future expenditures. This supports customers' interest in receiving cost-effective services that will help them economize their expenditures and thereby be (i) competitive in the case of private sector customers and (ii) reasonable with public (tax) funds in the case of public sector customers. Managing customer accounts by assessing – and sharing with the customer – aggregated information about usage allows the customers to more effectively manage expenses.

D. Continued

2. Compensation
   a. Data Processing is Proportionate and Does Not Prejudice Rights and Freedoms of Individuals

In processing data for compensation of both Microsoft's customer-facing workforce and our business partners based upon customer usage, Microsoft employs aggregated usage metrics, based on data already collected or generated through the customers' use of the services. Additional data is not collected solely for compensation, and Microsoft does not re-identify individuals from the pseudonyms that are employed. In addition, Microsoft does not permit access to the content of data that a customer places into the services when processing for compensation purpose.

As an example, the data processing employed to develop usage-based compensation may involve counting the number of users who have sent at least one email in a month (without identifying the users themselves), a metric that is used to understand whether users are activating and getting value from purchased products. This processing involves aggregating information at a product and tenant level, excluding any information about individual users. As such, this processing serves the strong interest of the customers in maximizing the efficacy of public or business expenditures, as described more fully below, while minimizing the processing of personal data to the extent necessary to achieve the customers' aims and avoiding privacy risks to individuals or interference with their data subjects' rights.

   b. Legitimate and Public Interests Bases

The goal of this business operation is to ensure that both Microsoft and partners have interests that are aligned with the customers, namely that the customers obtain maximum value. Microsoft has heard from public sector and enterprise customers around the world that they want to be billed based on their usage, not on a flat rate, so that they only pay for their products and services at a rate commensurate with their use. This goal is in line with the customers' interest in maximizing the efficacy of expenditures and the procurement of the best solutions for their objectives.

Microsoft has learned over time that in order to fully support our usage-based payment model, we need to provide usage metrics to our customer-facing personnel and business partners so they can have the customers' interests regarding usage as their key performance indicator as well. When personnel and business partners are rewarded not based solely on the sale of a product but based rather on the customers' actual use of products purchased, Microsoft's personnel and partners will be appropriately focused on developing a better understanding of the customers' needs and helping them target their purchases to those products that they will use most widely, and thus deliver the greatest value to the customers. For example, Microsoft can provide its personnel and business partners supporting the customers information on features that the customers are entitled to but are not using, in order to help the customers make choices about how to best use those features.

D. Continued

Ensuring that Microsoft personnel are focused on the customers' needs helps promote the customers' responsibility to maximize the efficacy of their expenditures and supports the customers' proper management and functioning by promoting the delivery of higher quality service.

3. Internal Reporting and Business Modelling
   a. Data Processing is Proportionate and Does Not Prejudice Rights and Freedoms of Individuals

Microsoft uses statistical data or data containing pseudonymous identifiers that has already been collected or generated through the customers' use of the services for internal reporting and business monitoring. This can be useful, for example, if Microsoft releases a new feature and wants to understand whether customers are having difficulty using it. That, in turn, can help Microsoft invest in improving features to make them more useful to the customers and other customers. Microsoft does not collect additional data solely for internal reporting and business modelling, and Microsoft does not re-identify individuals from the pseudonyms. Microsoft does not permit access to the content of data that a customer places into the services for internal reporting and business monitoring. Consistent with the goal of proportionality, this data is aggregated. In the majority of cases, usage data is aggregated across multiple customers instead of a single tenant because the focus of analysis is usage across customers generally or in market segments, e.g., number of users who use a given service capability, amount of usage on servers devoted to a specific online service, or adoption of a service capability in different market segments (e.g., small business, large organizations).

Accordingly, the combined effect of the strong technical and organizational controls avoids any privacy risk for individuals.

   b. Legitimate and Public Interests Bases

In the context of online services, Microsoft's offerings are not static. Rather, our customers rightly expect and instruct that our services evolve and improve to help our customers and their users be more productive in achieving their objectives and obtain more value for the expenditure of funds (public or private) on Microsoft's products. Microsoft's customers are better served by Microsoft improving services in ways that our internal metrics show are in practice appreciated by users.

Microsoft's internal reporting for such purposes as forecasting, capacity and business planning, and product strategy enables Microsoft to identify areas for product investment based on usage patterns for capabilities within the services, to develop pricing models that are sustainable for customers, partners, and Microsoft, and to plan future infrastructure investment to ensure we have the capacity to deliver services with the levels of performance and availability expected or required by customers. This supports the customers' interests in ensuring their service providers, including Microsoft, can continue to provide effective and efficient services to them.

D. Continued

4. Financial Reporting in Accordance with Legal and Stock Exchange Obligations

   a. Data Processing is Proportionate and Does Not Prejudice Rights and Freedoms of Individuals

To develop the information needed to meet its reporting obligations mandated by laws around the world, Microsoft processes personal data to build aggregate information across large segments of Microsoft's customers to report on the sales and adoption of these products to fully inform the market about Microsoft's business activities. This includes reporting Microsoft makes to the U.S. SEC.

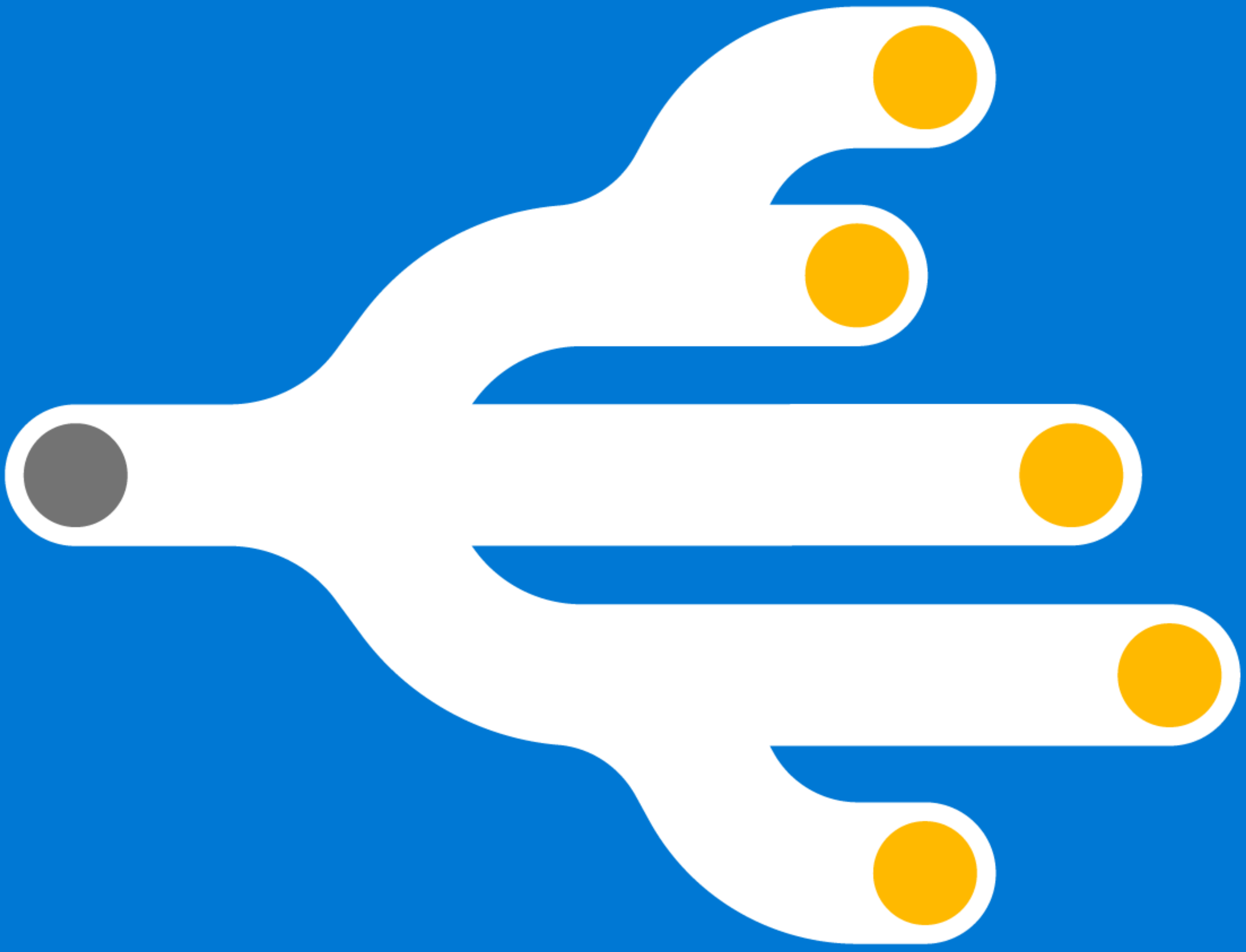
As with other processing by Microsoft described in this paper, the data processing deployed in this business operation is additional processing of data containing pseudonymous identifiers already collected or generated through the customers' use of the services; additional data is not collected for financial reporting; and Microsoft does not permit access to the content of data that a customer places into the services when processing for this purpose. To calculate reported usage metrics, Microsoft minimizes the use of personal data by aggregating it.

The processing initially starts with end user actions for the purpose of counting (for example, a system automatically generating reports on the number of users of a product within an organization must be able to recognise pseudonymous identifiers that distinguish one user from another so no users are double-counted), but the identifiers used are pseudonymized and the information is aggregated into counts that do not reflect any individual data subject's usage. Microsoft does not re-identify individuals from the pseudonyms. In addition, processing for purposes of financial reporting is expressly subject to limitations on disclosure of data under the DPA.

   b . Legitimate and Public Interests Bases

The public and legitimate interest justification for this processing flows from the responsibility that third parties (including Microsoft's competitors) and customers have for ensuring that service providers, including Microsoft, fulfil their obligations to comply with applicable laws and regulations designed to ensure the transparency and efficient functioning of markets. To advance these shared objectives, Microsoft is required to use data to provide transparency to the markets about its business activities.

Appendix A



Appendix A:

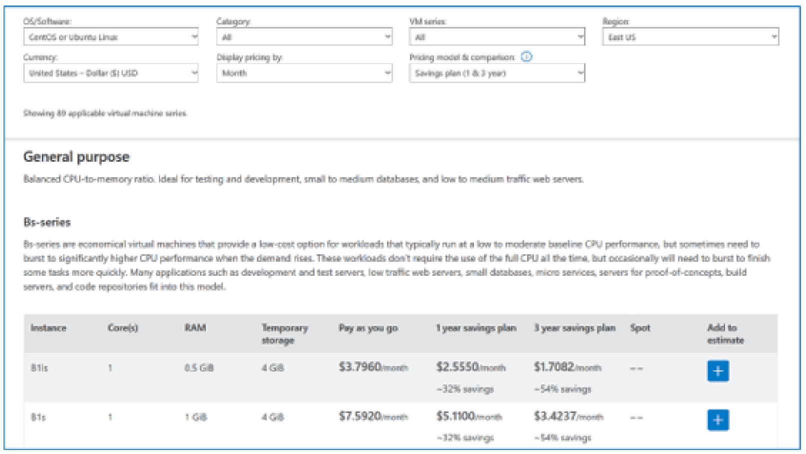
Examples demonstrating business operations in practice

Business operation 1: Billing and account management

Billing

Microsoft cloud services == Pay as you go

Needs to track and record who purchased, how services used, etc.



OS/Software: CentOS or Ubuntu Linux	Category: All	VM series: All	Region: East US
Currency: United States – Dollar ($) USD	Display pricing by: Month	Pricing model & comparison: Savings plan (1 & 3 year)	

Showing 89 applicable virtual machine series.

General purpose

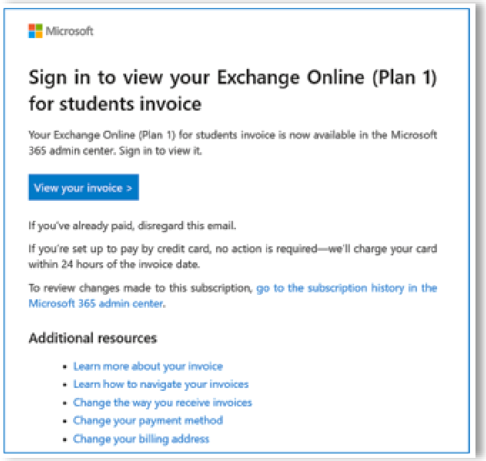
Balanced CPU-to-memory ratio. Ideal for testing and development, small to medium databases, and low to medium traffic web servers.

Bs-series

Bs-series are economical virtual machines that provide a low-cost option for workloads that typically run at a low to moderate baseline CPU performance, but sometimes need to burst to significantly higher CPU performance when the demand rises. These workloads don't require the use of the full CPU all the time, but occasionally will need to burst to finish some tasks more quickly. Many applications such as development and test servers, low traffic web servers, small databases, micro services, servers for proof-of-concepts, build servers, and code repositories fit into this model.

Instance	Core(s)	RAM	Temporary storage	Pay as you go	1 year savings plan	3 year savings plan	Spot	Add to estimate
B1ls	1	0.5 GiB	4 GiB	$3.7960/month	$2.5550/month ~32% savings	$1.7082/month ~54% savings	--	+
B1s	1	1 GiB	4 GiB	$7.5920/month	$5.1100/month ~32% savings	$3.4237/month ~54% savings	--	+

Azure Virtual Machine pricing example



Sign in to view your Exchange Online (Plan 1) for students invoice

Your Exchange Online (Plan 1) for students invoice is now available in the Microsoft 365 admin center. Sign in to view it.

If you've already paid, disregard this email.

If you're set up to pay by credit card, no action is required—we'll charge your card within 24 hours of the invoice date.

To review changes made to this subscription, go to the subscription history in the Microsoft 365 admin center.

Additional resources

- Learn more about your invoice
- Learn how to navigate your invoices
- Change the way you receive invoices
- Change your payment method
- Change your billing address

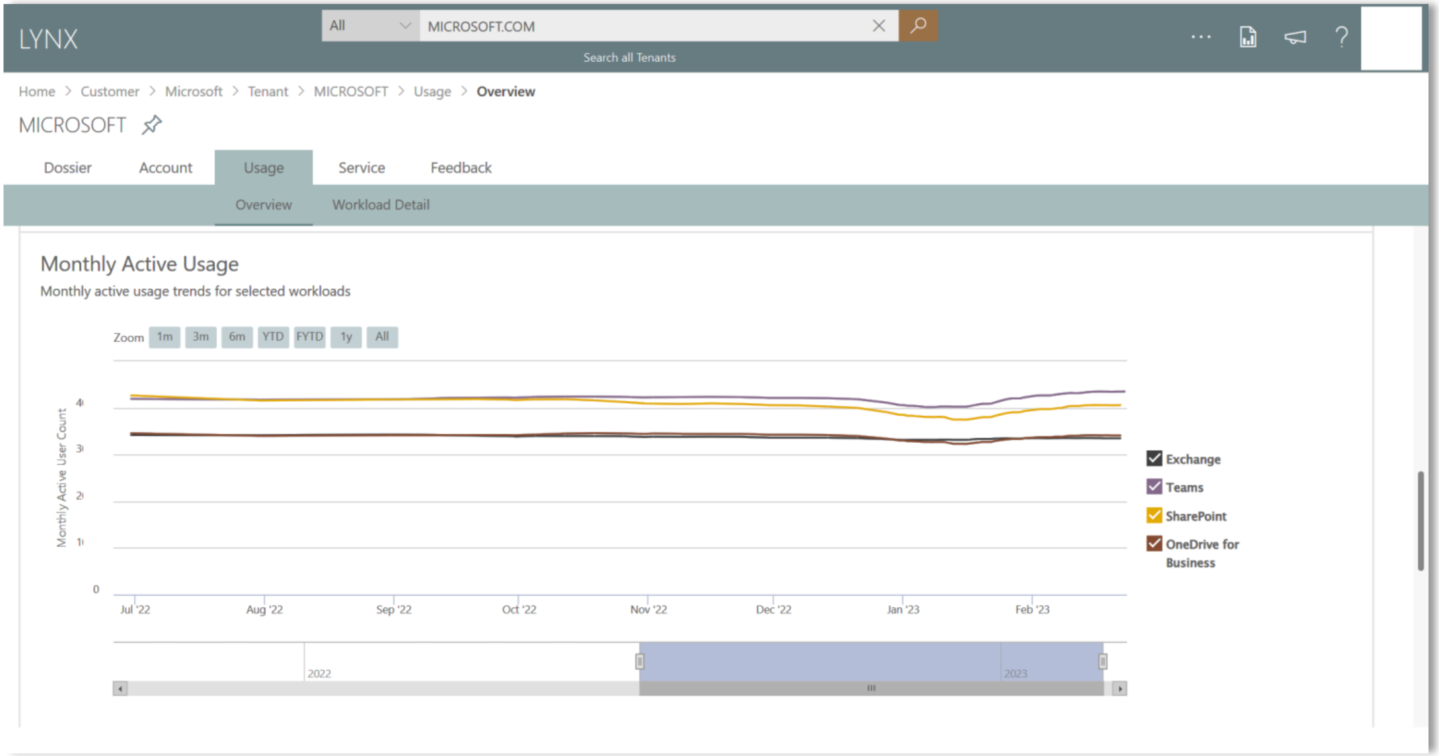
Example of invoice e-mail sent to Customer Admin

Appendix A:

Examples demonstrating business operations in practice

Business operation 2: Compensation

Example of tracking usage



No personal data but Organizational ID is included in aggregated usage data (e.g., Microsoft.com)

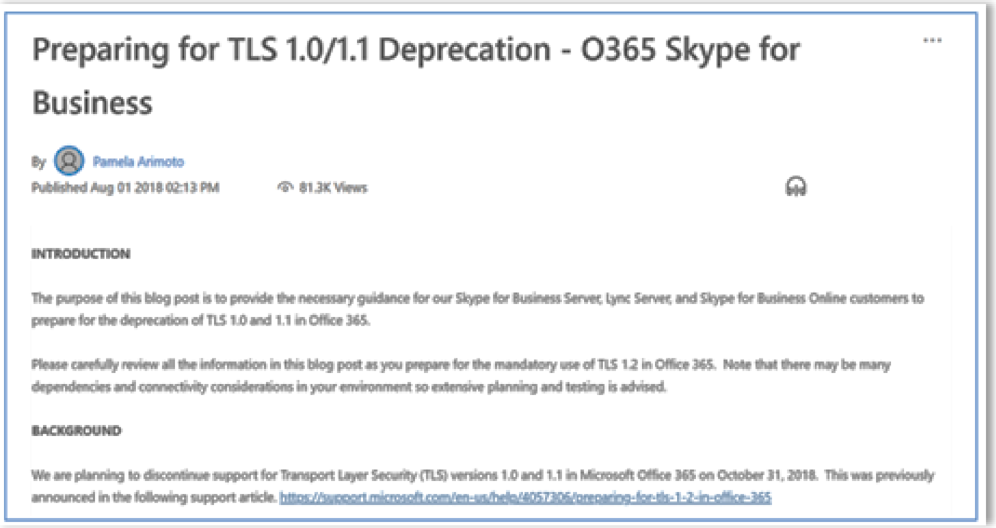
Appendix A:

Examples demonstrating business operations in practice

Business operation 3: Internal reporting and business modeling

Example 1: Usage-driven decision in product strategy

TLS1.0/1.1 depreciation was initially announced back in 2017-18



Preparing for TLS 1.0/1.1 Deprecation - O365 Skype for Business

By Pamela Arimoto
Published Aug 01 2018 02:13 PM 81.3K Views

INTRODUCTION

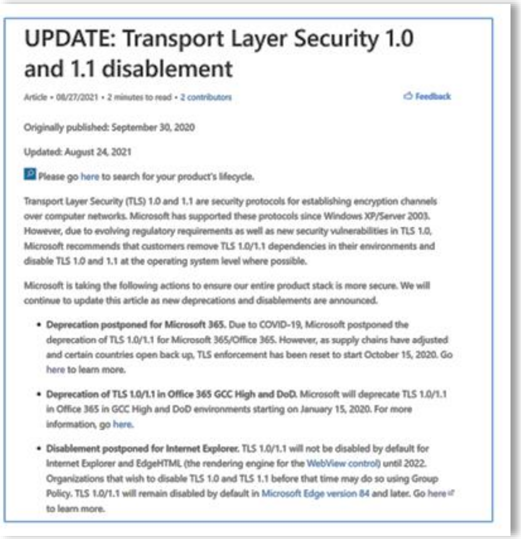
The purpose of this blog post is to provide the necessary guidance for our Skype for Business Server, Lync Server, and Skype for Business Online customers to prepare for the deprecation of TLS 1.0 and 1.1 in Office 365.

Please carefully review all the information in this blog post as you prepare for the mandatory use of TLS 1.2 in Office 365. Note that there may be many dependencies and connectivity considerations in your environment so extensive planning and testing is advised.

BACKGROUND

We are planning to discontinue support for Transport Layer Security (TLS) versions 1.0 and 1.1 in Microsoft Office 365 on October 31, 2018. This was previously announced in the following support article. https://support.microsoft.com/en-us/help/4057306/preparing-for-tls-1-2-in-office-365

With feedback from customers and usage data, Microsoft decided to postpone, and then re-started disablement



UPDATE: Transport Layer Security 1.0 and 1.1 disablement

Article • 08/27/2021 • 2 minutes to read • 2 contributors

Originally published: September 30, 2020

Updated: August 24, 2021

Please go here to search for your product's lifecycle.

Transport Layer Security (TLS) 1.0 and 1.1 are security protocols for establishing encryption channels over computer networks. Microsoft has supported these protocols since Windows XP/Server 2003. However, due to evolving regulatory requirements as well as new security vulnerabilities in TLS 1.0, Microsoft recommends that customers remove TLS 1.0/1.1 dependencies in their environments and disable TLS 1.0 and 1.1 at the operating system level where possible.

Microsoft is taking the following actions to ensure our entire product stack is more secure. We will continue to update this article as new deprecations and disablements are announced.

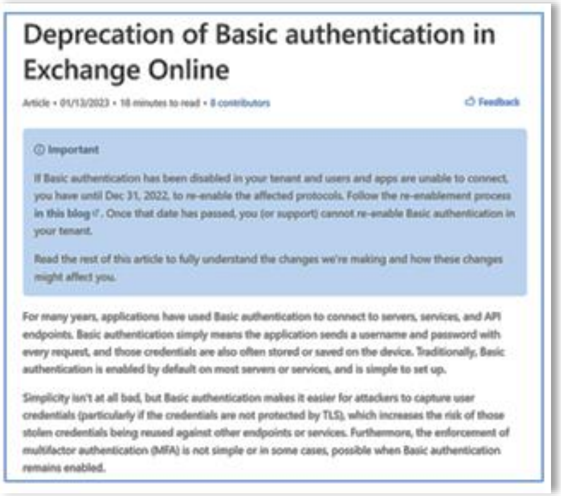
- **Deprecation postponed for Microsoft 365.** Due to COVID-19, Microsoft postponed the deprecation of TLS 1.0/1.1 for Microsoft 365/Office 365. However, as supply chains have adjusted and certain countries open back up, TLS enforcement has been reset to start October 15, 2020. Go here to learn more.
- **Deprecation of TLS 1.0/1.1 in Office 365 GCC High and DoD.** Microsoft will deprecate TLS 1.0/1.1 in Office 365 in GCC High and DoD environments starting on January 15, 2020. For more information, go here.
- **Disablement postponed for Internet Explorer.** TLS 1.0/1.1 will not be disabled by default for Internet Explorer and EdgeHTML (the rendering engine for the WebView control) until 2022. Organizations that wish to disable TLS 1.0 and TLS 1.1 before that time may do so using Group Policy. TLS 1.0/1.1 will remain disabled by default in Microsoft Edge version 84 and later. Go here to learn more.

Appendix A:

Examples demonstrating business operations in practice

Business operation 3: Internal reporting and business modeling

Example 2: Change gradually delivered per customer usage



Deprecation of Basic authentication in Exchange Online

Article • 01/13/2023 • 18 minutes to read • 8 contributors

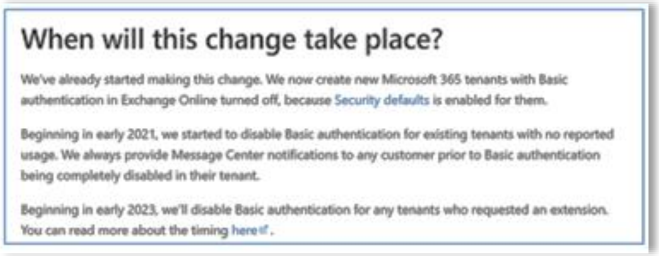
Important

If Basic authentication has been disabled in your tenant and users and apps are unable to connect, you have until Dec 31, 2022, to re-enable the affected protocols. Follow the re-enablement process in this blog. Once that date has passed, you (or support) cannot re-enable Basic authentication in your tenant.

Read the rest of this article to fully understand the changes we're making and how these changes might affect you.

For many years, applications have used Basic authentication to connect to servers, services, and API endpoints. Basic authentication simply means the application sends a username and password with every request, and those credentials are also often stored or saved on the device. Traditionally, Basic authentication is enabled by default on most servers or services, and is simple to set up.

Simplicity isn't at all bad, but Basic authentication makes it easier for attackers to capture user credentials (particularly if the credentials are not protected by TLS), which increases the risk of those stolen credentials being reused against other endpoints or services. Furthermore, the enforcement of multifactor authentication (MFA) is not simple or in some cases, possible when Basic authentication remains enabled.



When will this change take place?

We've already started making this change. We now create new Microsoft 365 tenants with Basic authentication in Exchange Online turned off, because Security defaults is enabled for them.

Beginning in early 2021, we started to disable Basic authentication for existing tenants with no reported usage. We always provide Message Center notifications to any customer prior to Basic authentication being completely disabled in their tenant.

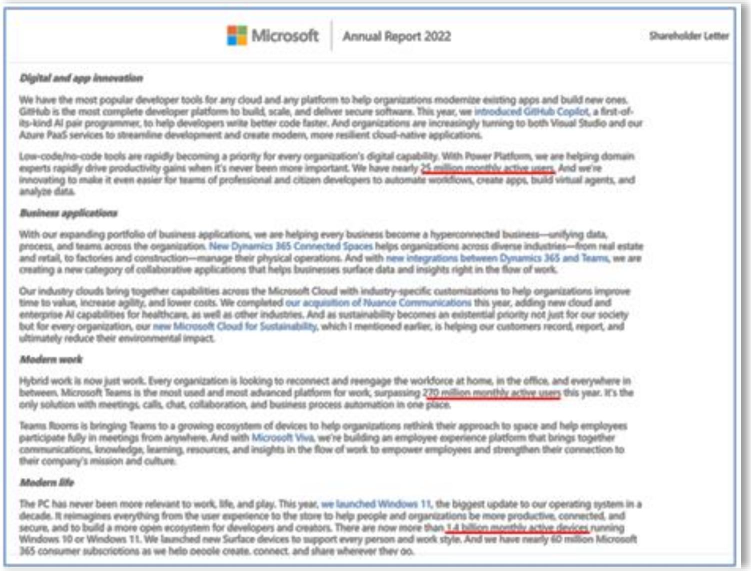
Beginning in early 2023, we'll disable Basic authentication for any tenants who requested an extension. You can read more about the timing here.

Appendix A:

Examples demonstrating business operations in practice

Business operation 4: Financial reporting

Financial reporting example



Microsoft | Annual Report 2022 Shareholder Letter

Digital and app innovation

We have the most popular developer tools for any cloud and any platform to help organizations modernize existing apps and build new ones. GitHub is the most complete developer platform to build, scale, and deliver secure software. This year, we introduced GitHub Copilot, a first-of-its-kind AI pair programmer, to help developers write better code faster. And organizations are increasingly turning to both Visual Studio and our Azure PaaS services to streamline development and create modern, more resilient cloud-native applications.

Low-code/no-code tools are rapidly becoming a priority for every organization's digital capability. With Power Platform, we are helping domain experts rapidly drive productivity gains when it's never been more important. We have nearly 25 million monthly active users. And we're innovating to make it even easier for teams of professional and citizen developers to automate workflows, create apps, build virtual agents, and analyze data.

Business applications

With our expanding portfolio of business applications, we are helping every business become a hyperconnected business—unifying data, process, and teams across the organization. New Dynamics 365 Connected Spaces helps organizations across diverse industries—from real estate and retail, to factories and construction—manage their physical operations. And with new integrations between Dynamics 365 and Teams, we are creating a new category of collaborative applications that helps businesses surface data and insights right in the flow of work.

Our industry clouds bring together capabilities across the Microsoft Cloud with industry-specific customizations to help organizations improve time to value, increase agility, and lower costs. We completed our acquisition of Nuance Communications this year, adding new cloud and enterprise AI capabilities for healthcare, as well as other industries. And as sustainability becomes an existential priority not just for our society but for every organization, our new Microsoft Cloud for Sustainability, which I mentioned earlier, is helping our customers record, report, and ultimately reduce their environmental impact.

Modern work

Hybrid work is now just work. Every organization is looking to reconnect and reengage the workforce at home, in the office, and everywhere in between. Microsoft Teams is the most used and most advanced platform for work, surpassing 270 million monthly active users this year. It's the only solution with meetings, calls, chat, collaboration, and business process automation in one place.

Teams Rooms is bringing Teams to a growing ecosystem of devices to help organizations rethink their approach to space and help employees participate fully in meetings from anywhere. And with Microsoft Viva, we're building an employee experience platform that brings together communications, knowledge, learning, resources, and insights in the flow of work to empower employees and strengthen their connection to their company's mission and culture.

Modern life

The PC has never been more relevant to work, life, and play. This year, we launched Windows 11, the biggest update to our operating system in a decade. It reimagines everything from the user experience to the store to help people and organizations be more productive, connected, and secure, and to build a more open ecosystem for developers and creators. There are now more than 1.4 billion monthly active devices running Windows 10 or Windows 11. We launched new Surface devices to support every person and work style. And we have nearly 60 million Microsoft 365 consumer subscriptions as we help people create, connect, and share wherever they go.