Microsoft

How does Microsoft handle your data in the cloud?

SUBPROCESSORS AND DATA PRIVACY

INTRODUCTION

Security, privacy, and compliance are core tenets of how we serve our customers and how we empower organizations to serve their customers. Since Microsoft operates in nearly every country in the world, we are subject to, and must operate consistent with, a multitude of laws, regulations, codes of conduct, industry-specific standards, and compliance standards. Microsoft also wears many hats—as a large international employer, as a provider of consumer products and services, and as an enterprise-class software and service provider.

Ensuring security in the processing of customer data stored and shared via the Microsoft Cloud is critical. We have decades-long experience building enterprise software and running some of the largest online services in the world. We use this experience to implement and continuously improve security-aware software development, operational management, and threat-mitigation practices that are essential to the strong protection of services and data. The purpose of this document is to outline the common security, privacy, and compliance questions customers have related to how Microsoft handles data that you share and store in the Microsoft Cloud, specific to the use of third parties.

SUBPROCESSORS: A SUBSET OF SUBCONTRACTORS

As one of the world's leading technology and cloud services providers, Microsoft relies on collaboration with and expertise of other companies to deliver innovative solutions that meet our customer's needs and keep our business running. When Microsoft utilizes the services of other companies, we refer to such third-party companies as suppliers or subcontractors. The risks typically associated with outsourcing, subcontracting, or subprocessing have been addressed and mitigated by minimizing where possible any single point of dependency on any supplier within our service.

When providing Cloud Services, Microsoft processes various categories of data, including customer data and personal data as defined by the Online Service Terms (OST). When Microsoft hires a supplier to perform work that may require the supplier to use or process such data in order to provide some aspect of the Online Services, they are identified as a "Subprocessor" (in accordance with the GDPR terminology), and they are disclosed in the Online Services Subprocessor list as discussed below. When hiring suppliers, Microsoft documents all the information security requirements for mitigating the risks associated with suppliers' access to the organization's assets.

TYPES OF SUBPROCESSORS

The Microsoft Online Services Subprocessor List provides a list of subprocessors that may have access to both customer data and personal data. There are different types of subprocessors used, as described below.

Technology: These subprocessors provide technologies used to deliver specific Microsoft Online Services. If you deploy one of these services, the subprocessors identified for that service may process, store, or otherwise access customer data or personal data in the course of helping to provide that service. Should these subprocessors fail in their duties, the service they work for may suffer a loss of availability.

Ancillary: These subprocessors provide ancillary services to help support, operate, and maintain the Online Services. In such cases, the subprocessors identified may process, store, or otherwise access limited customer data or personal data in the course of providing their ancillary services. Should these subprocessors fail in their duties, they may impact a feature of a larger service.

Staff Augmentation: These subprocessors provide contract staff that work in close coordination with Microsoft employees to help support, operate, and maintain the Microsoft Online Services and in the course of doing so may be exposed to customer data or personal data. In all such cases, customer data or personal data resides only in Microsoft facilities, on Microsoft systems, and subject to Microsoft policies and supervision. For example, a subprocessor may perform remote troubleshooting on a Microsoft server and in the course of doing so may be exposed to snippets of customer data in a server crash dump log. Activities of these subprocessors related to online services are in scope for applicable third-party audits.

POTENTIAL TO ACCESS DATA

So, if a subprocessor has "potential to access" customer or personal data, does that mean they're looking at your data? While all the subprocessors included on the list have the potential to access customer data or personal data (or both), in practice, the actual access to data is much less. In many cases, the data is pseudonymized and the vendor personnel do their work without ever needing to access non-anonymized data. In other cases, the tasks the vendor personnel perform do not themselves require access to data, but they technically have potential to do so.

In a highly secure, access-controlled environment, subprocessors may have the potential to access restricted data such as customer and/or personal data specifically to deliver functions in support of online services that Microsoft has hired them to provide, and they are prohibited from using this data for any other purpose. All subprocessors are required to maintain top security and confidentiality of customer and personal data and are contractually obligated to meet strict privacy and security requirements that are equivalent to or stronger than the contractual commitments Microsoft makes to its customers in the Online Services Terms. Subprocessors are also required to meet GDPR requirements, including those related to implementing appropriate technical and organizational measures to protect personal data.

TYPES OF DATA SHARED WITH MICROSOFT

As specified in contractual commitments to its customers, Microsoft defines customer data as all the data the customer provides to Microsoft through their use of Microsoft business cloud services. Some customer data is also deemed personal data, as defined under the GDPR. Microsoft also processes some personal data generated or collected through the operation of the online services that is not contained within the scope of customer data.

CUSTOMER DATA is all data, including text, sound, video, or image files and software, that you provide to Microsoft or that is provided on your behalf through your use of Microsoft online services. For example, it includes data that you upload for storage or processing, as well as applications that you upload for distribution through a Microsoft enterprise cloud service.

PERSONAL DATA means any information relating to an identified or identifiable natural person. In other words, personal data is any data that is associated with a specific person. Personal data provided by our customers through their use of online services, such as the names and contact information of customer end users, would also be considered customer data. But personal data could also include certain data that is not customer data, such as the user ID our service assigns to each user; such personal data is pseudonymized to prevent identification of the individual.

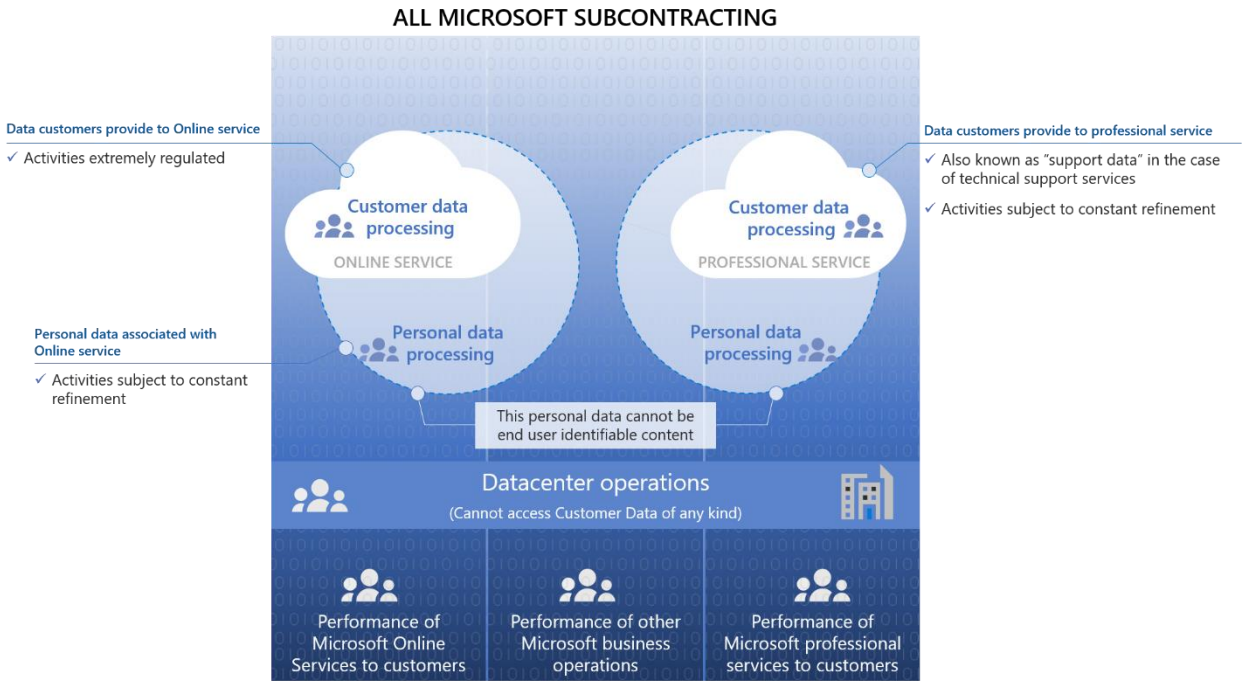
PUBLIC DISCLOSURE OF MICROSOFT SUBPROCESSORS

The Microsoft Online Services Subprocessor List discloses all suppliers that are security cleared and authorized to process customer data or personal data within Microsoft online services. This list is applicable for all Microsoft online services governed by the Online Services Terms for which Microsoft is a data processor. As of September 5, 2019, Microsoft has simplified and radically reduced the number of

subprocessors with the potential to access customer data or personal data. This shortened list helps customers conduct a better risk assessment with a better outcome for their regulators and their business.

Microsoft publishes the names of any new subprocessors to this list on the Service Trust Portal six months in advance of the subprocessor's authorization to perform services that may involve secure access to customer data or fourteen days in advance of potential access to personal data within Microsoft online services. This advance notice enables customers to investigate the subprocessor, perform a risk assessment, and ask questions of Microsoft about the subprocessing engagement. As mentioned in the Online Services OST, if a customer does not approve of a new subprocessor, then the customer may terminate any subscription for the affected online service without penalty by providing, before the end of the relevant notice period, written notice of termination that includes an explanation of the grounds for non-approval.

To receive notifications of updates to the subprocessor list, you can use the My Library functionality recently launched on the Service Trust Portal. Through My Library, you can access and review relevant documents, and set up specific notifications for updates to those documents. For Professional Services, please refer to the Microsoft Trust Center for instructions on how to access the subprocessor list.



Graphical representation of Microsoft subcontracting and data subprocessing

MICROSOFT GOVERNANCE OF SECURITY AND PRIVACY STANDARDS

Microsoft has a robust supplier management program, which includes a code of ethics, training requirements, and a stringent set of security and privacy requirements that are audited specifically for a small set of security cleared vendors. This robust supplier management program also includes the Microsoft code of ethics and training requirements specific to the services provided by the subcontractor or subprocessor. This starts with the Supplier Code of Conduct (SCoC) and its accompanying training which outlines the expected behavior of Microsoft employees and anyone doing business with Microsoft.

Before any supplier can engage in any work with Microsoft, they must enter into a Master Supplier Services Agreement (MSSA) with Microsoft. In addition to ensuring structure and uniformity to all business transactions between Microsoft and the supplier, this overarching agreement dictates terms related specifically to privacy and data protection on the part of suppliers working with Microsoft customer and personal data. For example, the MSSA stipulates that suppliers engaged in subprocessing personal data can only do so on documented instructions from Microsoft, including with regard to transfers of personal data to outside entities like international organizations (unless required to do so by EU or Member State law, and having advised Microsoft of this legal necessity prior to processing), and processing of any personal data is limited to the defined scope of the request from Microsoft. Any individuals authorized to process personal data have committed themselves to confidentiality, take all measures required in accordance with good industry practice and applicable data protection law, and do not subcontract work out to additional parties without prior authorization and strict adherence to the same security standards.

Subprocessors who have the potential to access to customer data and personal data are subject to heightened requirements. A stipulation of the MSSA and requirement for all subprocessors is that they join the Microsoft Supplier Security and Privacy Assurance Program (SSPA). This program is designed to standardize and strengthen data handling practices by setting privacy and security requirements for Microsoft suppliers, and to drive compliance to these requirements to ensure supplier business processes and systems are consistent with those of Microsoft. Participating suppliers maintain their status in the program by attesting annually or more often to their compliance with the Supplier Data Protection Requirements (DPR) outlined by the program.

In the case of suppliers who perform staff augmentation work, the same controls in place for data access such as credentials, "just in time access", and "just enough access" will apply to the contract staff as they do for a Microsoft full time employee. Additionally, subcontractors who work in facilities or on equipment controlled by Microsoft are contractually obligated to follow our privacy standards and undergo regular privacy training.

In addition to the baseline requirements provided in the SSPA, Microsoft makes added commitments. These additional privacy and security commitments are documented in the following areas:

- Privacy, Security, and Data Protection Addendum
- Background Check Addendum
- EU Model Clause Addendum
- Enhanced Security & Audit requirements

These terms reflect commitments that Microsoft has made to its customers and are required for any supplier with access to customer data.

ALIGNMENT WITH THE GDPR AND EU MODEL CLAUSES

In order to provide a greater level of assurance, Microsoft complies with both international and industry-specific compliance standards and participates in rigorous third-party audits that verify our security controls. As required by the GDPR, Microsoft implements and maintains appropriate technical and organizational security measures, including measures that meet the requirements of ISO 27001 and ISO 27018, to protect personal data it processes as a data processor or subprocessor on its customers' behalf.

Additionally, Microsoft follows the EU Standard Contractual Clauses and US-EU and Swiss-US Privacy Shield Frameworks, which are included in the Online Services Data Protection Addendum. It's important to note that the EU Standard Contractual Clauses we offer are specifically designed to provide safeguards for

data transfers from controllers in the EU to data processors established outside EEA. For the Online Services, Microsoft is a data processor (or subprocessor) acting on our customers' behalf to process Customer Data, Support Data, and Personal Data.

INDUSTRY SPOTLIGHT: EUROPEAN BANKING AUTHORITY (EBA) GUIDELINES

Another example of heightened assurance is that Microsoft follows strict European Banking Authority (EBA) recommendations. The EBA is "an independent authority that works to ensure effective and consistent prudential regulation and supervision across the EU banking sector." In December 2017, the EBA issued its Final Report: Recommendations on outsourcing to cloud services providers, which included substantive input from Microsoft and outlined a comprehensive approach to the outsourcing of cloud computing by financial institutions in the EU.

The EBA Guidelines, which took effect on September 30, 2019, clarify that outsourcing to cloud service providers is permitted, apply a principles-based approach towards measuring risk from a technology-neutral perspective, and strive towards greater harmonization within Europe and beyond. These guidelines apply to credit institutions and investment firms, as well as payment and electronic money institutions.

To help financial institutions in the EU follow the European Banking Authority (EBA) guidelines for cloud adoption, Microsoft published European Banking Authority Guidance Addresses Cloud Computing for the First Time. This document addresses key requirements and explains how Microsoft online services can be used to satisfy them. The guidance can help financial institutions adopt Azure and Microsoft 365 with the confidence that they can meet their obligations under the EBA framework.

The Microsoft guidance addresses, point by point, each of the EBA recommendations:

- **Audit rights.** Microsoft provides contractual audit rights for customers and rights of examination for regulators in its industry-leading Financial Services Amendment.
- **Notification regarding outsourcing.** Microsoft can assist customers with notifying regulators of material activities to be outsourced.
- **Data residency.** With 54 regions, including six in Europe, Microsoft offers the largest number of datacenters worldwide of any cloud service provider. Organizations can deploy workloads in one region without being required to host data in Europe.
- **Notification regarding subprocessors.** Microsoft leads the industry with a contractual commitment to provide customers with six months notice of new subprocessors, and a right to terminate if the customer does not approve of the appointment of a new subprocessor.
- **Business continuity.** Microsoft provides business continuity and resolution provisions in our Financial Services Amendment, including the willingness to provide transition assistance through Microsoft Consulting Services.
- **Risk assessment and security monitoring.** Microsoft enables customers to conduct their own risk assessments and provides tools and dashboards so they can supervise and monitor our cloud services.

For financial institutions in the EU, Microsoft has also published Risk Assessment and Compliance Guide for Financial Institutions in the Microsoft Cloud, a checklist modeled in accordance with the EBA guidance. It explains how to establish a governance model optimized to meet regulatory requirements, and efficiently evaluate the risks of using Microsoft cloud services, followed by submission for regulatory approval. Our guide includes a list of questions to be answered in a regulatory submission that are drawn from, and responsive to, EBA guidance on outsourcing to cloud service providers.

Additional learning

Microsoft in-scope cloud services and how to implement:

- Azure
- Microsoft 365
- Response to EBA guidance: Microsoft guidance helps EU financial institutions follow EBA recommendations for cloud adoption.
- Financial use cases: Use case overviews, tutorials, and other resources to build Azure solutions for financial services.
- Financial Services Compliance Program: Financial institutions can get help assessing the risks of using Microsoft cloud services.

WHAT ACTIONS SHOULD YOU TAKE?

Every organization's needs are unique, from your level of risk tolerance to the regulations applicable to your specific industry or region. As such, you are in the best position to define what is and is not deemed a business-critical operation. We recommend that you take the time to develop and refine your own internal governance processes to monitor and manage the data processing you outsource to suppliers (including Microsoft). In reviewing Microsoft's use of subprocessors, we recommend the following actions and considerations:

- Subscribe to notifications for any changes to the Microsoft subprocessor list. Be sure to keep records of revised lists as needed to aid in your risk assessment decision making.
- Understand that use of certain Microsoft online services means use of the subprocessors associated with providing that service. You may opt out of using specific services, but understand that removal of some elements may impact the overall value of Microsoft online services.
- While reviewing the list of subprocessors, determine whether the services impacted are relevant to your business or are considered business critical operations. Refer to your internal governance processes to determine your acceptable level of risk while considering the value provided by the services (i.e. Multi-Factor Authentication or IaaS building blocks).

Should you have concerns about a new subprocessor, please raise these concerns with your Microsoft account team. Your account team is available to answer questions, provide guidance, and help you resolve issues that may impact your use of Microsoft online services.

For additional guidance on developing an internal governance process, see Risk Assessment and Compliance Guide for Financial Institutions in the Microsoft Cloud.

RESOURCES TO LEARN MORE

Review these additional resources for more details on how Microsoft works with and protects your customer data.

Data collection information: Learn about the kinds of data we collect.

Microsoft Trust Center | Data Access: Learn more about who can access your data and on what terms.

Microsoft Online Services OST: Review the licensing terms, conditions, and supplemental information relevant to the use of Microsoft online services.

Microsoft Online Services Data Protection Addendum: Review additional details on how Microsoft follows the EU Standard Contractual Clauses and US-EU and Swiss-US Privacy Shield Frameworks.

Microsoft Online Services Privacy Statement: Learn about the personal data Microsoft processes, how we process it, and for what purposes.

Restricted Access to Customer Data: Learn how Microsoft business cloud services take strong measures to help protect data from unauthorized access and inappropriate use.

Microsoft licensing terms and documentation: Access licensing terms, conditions, and supplemental information relevant to the use of products and services licensed through Microsoft Volume Licensing programs.

Additional sites to explore

- Microsoft Service Trust Portal
- Microsoft Financial Services Compliance Program
- Microsoft business cloud services and financial services
- Financial services compliance in Azure
- Azure Financial Services Cloud Risk Assessment Tool
- Microsoft Financial Services Blog
- Compliance on the Microsoft Trust Center