Microsoft

Trusted data protection

Microsoft Online and Professional Services

Overview

Cloud computing is growing in popularity and adoption, but many organizations have questions about trust and data protection. As more content moves to the cloud—versus being stored locally, where organizations carried the majority of the burden of ensuring data protection—data handling and storage practices are critical in the selection of a cloud service provider. You need to be assured you can trust the data protection of a cloud service provider. Clearly understanding how Microsoft Online and Professional Services classifies, processes and protects organizational data and how we help your organization comply with a number of national, regional and industry- specific requirements is fundamental to the evaluation and migration to the services.

This guide highlights how Microsoft Online and Professional Services classifies, processes and protects data. It provides a summary and is an easy reference to additional and more detailed information on the spectrum of topics ranging from data categorization, location, transfers, limitations of use of the data we process. It's also suggested that you consult the Microsoft Online Services Terms (OST) and Data Protection Addendum (DPA) if there are very discrete questions you or your organization have.

Contents

Your data is just that, your data.

We use your data to provide the services you pay for.

We don't share, mine or use it for advertising purposes.

Your data always belongs to you.

You can access, modify or delete it at any time.

- When you use our cloud, you get the benefits of a multitenant service and the peace of mind that we keep your customer data confidential and respect your privacy.
- We only use your customer data to provide the services you pay for.
- We offer you the flexibility to configure and use our services in a manner that best meet your privacy needs.

We give you the benefits of a multitenant service with assured confidentiality

With Microsoft Online Services, our business is to safely process your organization's most valuable digital asset – your data. Your business is your business. We do not mine or use your customer data for marketing or advertising and we do not share it with Microsoft advertiser-supported services. We also believe that any third-party requests for your data by law enforcement, governments or civil litigants should be addressed directly to you. For information on how we handle such requests, see here.

To assure the confidentiality of your data, we process it separately from data that Microsoft processes to run its consumer businesses (businesses such as Xbox, free mail services, web browsers and search engines). We also use logical isolation to segregate the storage and processing for each of our multitenant customers to help ensure that your data is not combined with our other enterprise customers' data.

Categories of data that we process

Data that is used throughout the lifecycle of your account to provide you with Microsoft Online Services or Professional Services falls within one of four separate and distinct data categories:

- customer data
- service generated data
- diagnostic data
- professional services data

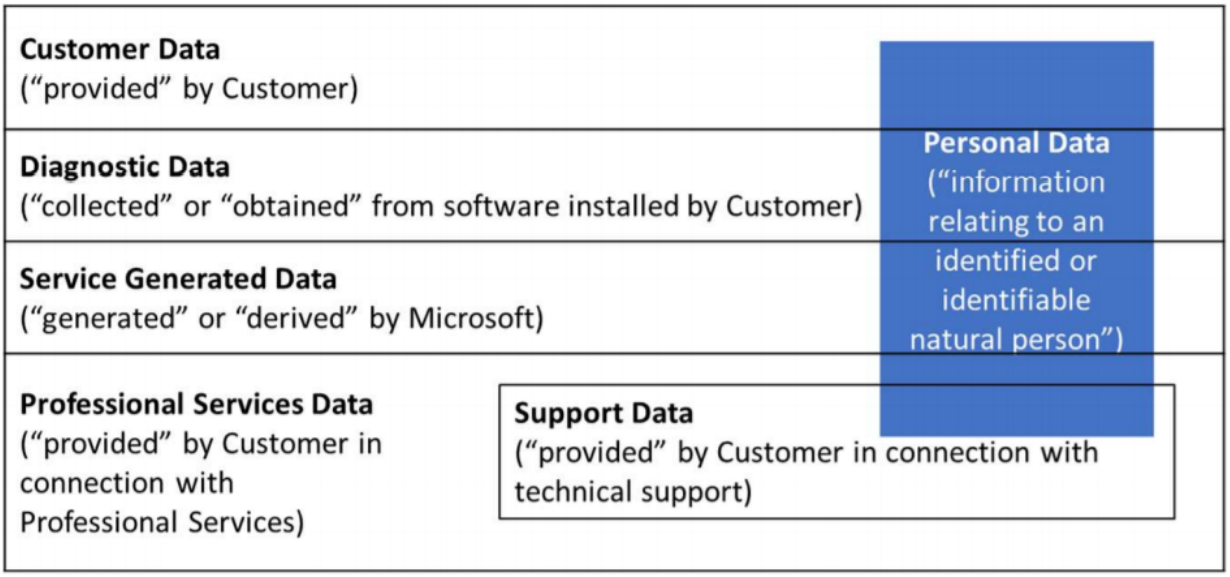
Customer data and professional services data are data that you provide to Microsoft. Service generated data is generated by our systems. Diagnostic data is data we collect from locally installed software. Definitions and examples for each of these data categories can be found here.

When you use Microsoft Online Services, three of the above four data categories are processed -- your customer data, service generated data and diagnostic data. When you use Professional Services, we only process professional services data and any other data that you authorize us to access in order to perform the professional services requested.

Data from each of these four data categories are also used to perform a limited set of legitimate business operations (LBOs) that are incident to delivering Microsoft Online Services and Professional Services. These LBOs are enumerated in the section below.

How we limit our use of the data we process

To comply with broadly applicable privacy laws such as GDPR, we strictly limit our use of all personal data within the four categories of data processed. To protect the confidentiality of your business data, we further strictly limit the use of all customer data, and all professional services data. We do not access your data to determine what is personal or not. Instead, we assume that all customer data and all professional services data contain personal data.



We use the GDPR definition for personal data, which is defined here. The blue box in the above illustration helps to convey that personal data can be a subset of each of the four categories of data processed. Personal data within diagnostic data and service generated data are mostly in the form of unique machine-generated numbers that are linkable to users.

Data used to provide Microsoft Online Services. When use you use the Online Services, all customer data and all personal data within the data we generate (diagnostic data and service generated data) are used to:

- Deliver functional capabilities as licensed, configured, and used by you and your users, including providing personalized user experiences.
- Troubleshoot (preventing, detecting, and repairing problems).
- Provide ongoing improvements (installing the latest updates and making improvements to user productivity, reliability, efficacy, and security).

Data used to provide Professional Services. When you use Professional Services, all professional services data is used to:

- Deliver the Professional Services, including providing technical support, professional planning, advice, guidance, data migration, deployment, and solution/software development services.
- Troubleshoot (preventing, detecting, investigating, mitigating, and repairing problems, including Security Incidents).
- Provide ongoing improvement (maintaining the Professional Services, including installing the latest updates, and making improvements to the reliability, efficacy, quality, and security).

We do not use your professional services data to provide Professional Services for other customers. However, other customers may benefit from the issues we troubleshoot for you. For example, if you

report a problem with an Azure Service, the same problem experienced by other customers may automatically be fixed when the problem is fixed for you.

Data used to support our ability to provide you with Microsoft Online and Professional Services. We also process data from the above four data categories to perform a limited set of legitimate business operations (LBOs) that may be needed to support our ability to provide you with Microsoft Online Services and Professional Services. With limited exceptions (i.e., to combat fraud and comply with legal obligations), we limit our use of personal data for LBOs by using only pseudonymized data originating from diagnostic data and service generated data, and aggregating this data prior to using it for LBOs such that it is no longer linkable back to users.

Our use of data to perform LBOs is limited to the following functions:

(1) billing and account management

(2) compensation (e.g., calculating employee commissions)

(3) internal reporting and modeling (e.g., forecasting, revenue, capacity planning, product strategy)

(4) combatting fraud, cybercrime, or cyber-attacks that may affect Microsoft or Microsoft Products

(5) improving the core functionality of accessibility, privacy or energy-efficiency

(6) financial reporting or compliance with legal obligations

During the lifecycle of your account

At all times during the term of your subscription, you can access, rectify, restrict the processing of, delete and export your customer data stored in our cloud. You can also access, extract and delete personal data that may be in service-generated and diagnostic data except for data that may compromise the security or stability of the service. You do not have the ability to restrict the processing of or rectify the data that Microsoft generates because this data constitutes a historical record of actions taken in the cloud, and preserving the integrity of this record is critical to protecting our customers from fraud and compromises to security. If you would like to perform any of these functions to meet a data subject request, we have detailed documentation for each of our Online Services to assist you. See Data Subject Requests and the GDPR and CCPA. For more GDPR-specific information, see the compliance and GDPR section of this article here.

At the end of your subscription

When you leave your subscription, Microsoft will retain your customer data in a limited function account for 90 days so you can extract the data. After this 90-day retention period, we will delete your customer data within 90 days unless we are authorized to retain it or required to retain it by law. We

also delete all service-generated and diagnostic data as part of our standard Microsoft data life cycle, unless needed to maintain the security and stability of our services.

We provide you with increased transparency and control over your data.

Customers in different industries have different compliance needs. Our Online Services are designed to permit you to configure the service to best meet your organization's goals. Some Online Services permit you to allow your users to elect to use add-ins or connected services with terms of use other than the Online Service Terms. Our services have built in controls that allow you to enable or disable these optional connected services. Our services also enable you to limit or change the diagnostic data levels that we collect from locally installed M365 Apps, and we plan to add similar diagnostic data controls for other major apps, including the thin client for Microsoft Teams, that connect to Microsoft clouds. For more information about this commitment, see The Microsoft Privacy Report, which is updated twice a year.

You create amazing content. We protect and secure it.

No matter which Online Services you use, we make it easy for you to create, store, and share your content with peace of mind. We protect your data with state-of-the-art technology and operations.

- Your data is protected every step of the way.
- We operate our services with zero standing access to customer data.
- We are transparent about which subprocessors we use that have access to customer data and personal data and the stringent set of security and privacy requirements they must meet.
- We abide by all applicable data transfer and data protection laws.

Data Protection

Customer data is encrypted in transit and at rest. Microsoft uses industry standard technologies such as TLS to encrypt all data in transit between users' devices and Microsoft datacenters, and between Microsoft datacenters. This includes messages, files, meetings, and other data. Enterprise data is also encrypted at rest in Microsoft datacenters. For more information about encryption-at-rest, see these articles for Azure, Dynamics 365 and Office 365.

Data Location

We offer an ever-expanding network of datacenters across the globe to make sure your data stays close to home, whenever possible. We do not control or limit the locations from which you or your users may access, copy, or move customer data. For data location information specific to each Online Service, go to Cloud service data residency and transfer policies on the Trust Center and select "expand all."

Infrastructure protection and breach notification commitment

Microsoft implements and maintains appropriate technical and organizational measures to protect your customer data, professional services data and personal data. These measures protect against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to the data when transmitted, stored or processed.

A guiding principle of our security strategy is to "assume breach." We emphasize and deeply invest in monitoring, early detection and rapid response efforts in order to identify potential threats and to reduce and mitigate the impact of any breach. Our global incident response team works continually to

mitigate the effects of any attack against our cloud services. Breaches that expose personal information can have serious consequences. For many organizations, government and industry regulations require that you protect the privacy of certain types of data. If we become aware of a breach of security that results in unauthorized access, destruction, loss, alteration, or disclosure of your customer data or any personal data, Microsoft will:

- Promptly notify you of the security incident.
- Investigate the security incident and provide you with detailed information about it.
- Take reasonable steps to mitigate the effects and to minimize any resulting damage.

You can read more about Breach Notification and related articles here.

Data Access

We take strong measures to protect your data from inappropriate access, including restrictions that limit access for Microsoft personnel and subprocessors. The operational processes that govern access to customer data in Microsoft Online Services are protected by technical and organizational measures that include strong authentication and access controls, both physical and logical. We proactively audit access controls at all layers of our services. Our services are designed to allow Microsoft's engineers to operate and maintain the service without accessing customer data. Microsoft employees have no standing access to customer data, including customer data, and no privileged access to the production environment. When access is required for service operations, role-based access controls are used to ensure that the access is for an appropriate purpose, for a limited time, and approved with management oversight.

Transparency and Controls Over Subprocessors

Microsoft shares data with third parties acting as its subprocessors to support functions such as customer and technical support, service maintenance, and other operations. Subprocessors can only access and use customer data to deliver the services they were hired to provide. All subprocessors 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 Data Protection Terms. You can view the Microsoft Online Services Subprocessor List which identifies subprocessors authorized to subprocess customer data or personal data in Microsoft Online Services. This whitepaper on subprocessors explains the type of data Microsoft's suppliers can access and Microsoft's robust supplier management program.

Data Transfers

We also comply with the below international data protection laws regarding transfers of customer data across borders.

EU Model Clauses

EU data protection law regulates the transfer of EU customer personal data to countries outside the European Economic Area (EEA). Microsoft EU Standard Contractual Clauses provide specific contractual guarantees around transfers of personal data that Europe's privacy regulators have determined meet EU standards for international transfers of data. All transfers of customer data and personal data out of the European Union, European Economic Area, United Kingdom, and Switzerland are governed by these Standard Contractual Clauses.

EU-U.S. Privacy Shield

Microsoft is certified to the EU-U.S. Privacy Shield Framework and the commitments they entail. However, Microsoft no longer relies on the EU-U.S. Privacy Shield Framework as a legal basis for transfers of personal data out of the EU in light of the judgment of the Court of Justice of the EU in Case C-311/18.

Your regulatory needs are our priority.

Our services are designed to support your ability to comply with a vast array of national, regional and industry-specific requirements. Don't just take our word for it. Our services are subjected to rigorous third-party audits.

- We support an expansive set of compliance offerings to help you meet regulatory and compliance responsibilities.
- We provide the assistance you need to comply with GDPR.
- We know that your compliance needs constantly evolve. We proactively engage globally with our customers, governments, regulators, standards bodies and non-governmental organizations to understand emerging regulatory cloud requirements and ensure our ability to support them.

Our shared responsibility model

While it is up to you to determine whether Microsoft Online Services comply with the specific laws and regulations that are applicable to your business, we help you make these assessments, by providing the specifics of our compliance programs, including audit reports and compliance packages. Your auditors can compare Microsoft results with your own legal and regulatory requirements, and you can verify the implementation of controls by requesting detailed audit results and reports, many of which are free to customers and trial customers through the Service Trust Platform. To the extent that your audit requirements cannot reasonably be satisfied through audit reports, documentation or compliance information that is generally available to customers, you as a customer also have the right to audit us at your own expense. How you can exercise these rights are detailed in the "Auditing Compliance" section of the DPA.

Compliance offerings

We engage globally recognized audit firms to certify the compliance of our online services against dozens of international standards and sector-specific requirements on a regular basis. Through these intensive audits, we obtain certifications for Microsoft Online Services that span a diverse set of areas – from core security to healthcare to specific government requirements. For a full list of our certifications, including a list of all services that are in scope for these certifications, see Microsoft Compliance Offerings. Our key certifications include the following standards and compliance regimes:

- **ISO/IEC 27001** – ISO/IEC 27001 is an international security standard that formally specifies an Information Security Management System (ISMS) intended to bring information security under explicit management control. This formal specification was developed by the International

Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) to mandate requirements that define how to implement, monitor, maintain, and continually improve an organization's ISMS. It also prescribes a set of best practices that include documentation requirements, divisions of responsibility, availability, access control, security, auditing, and corrective and preventive measures. Certification to ISO/IEC 27001 helps organizations comply with numerous regulatory and legal requirements that relate to the security of information.

- **Service Organizational Controls ("SOC") –** SOC is a control framework that safeguards the confidentiality and privacy of information stored and processed in the cloud. The SOC audit provides independent validation that O365's service commitments and system requirements relevant to security, availability, processing integrity, and confidentiality are achieved and that the controls governing our service are operating effectively. Developed by the American Institute of Certified Public Accountants (AICPA), this framework aligns with the International Standard on Assurance Engagements (ISAE), the reporting standard for international service organizations. The Statement on Standards for Attestation Engagements No. 18, the International Standards for Assurance Engagements No. 3402 and, in Germany, the IDW 951, are the standards under which the SOC 1 audit is performed. A SOC 2 audit, which corresponds to ISAE 3000, gauges the effectiveness of a cloud service provider's system based on the AICPA Trust Service Principles and Criteria.

- **U.S. Federal Risk and Authorization Management Program (FedRAMP)** – FedRAMP provides a standardized approach for assessing, monitoring, and authorizing cloud computing products and services under the U.S. Federal Information Security Management Act (FISMA) and to accelerate the adoption of secure cloud solutions by federal agencies. All U.S. federal agencies use FedRAMP to validate the security of cloud services.

- **U.S. Department of Defense Cloud Computing Security Requirements Guide (DoD SRG)** – To facilitate utilization of cloud services the U.S. Department of Defense (DoD) developed the DoD Cloud Computing Security Requirements Guide (DoD SRG). The SRG defines the baseline security requirements for cloud service providers that host DoD information, systems, and applications, and for DoD's use of cloud services.

Note: Although FedRAMP and DoD SRG audits apply only to the U.S. Government instance of Microsoft's cloud services, Microsoft applies similar controls across all instances of our cloud and uses the same software across all instances. Where there are controls specific to the United States (such as U.S. citizen requirements) these are only applied in the U.S. Government instances of Microsoft's cloud services.

Need to comply with GDPR? We've got you covered.

The European Union's General Data Protection Regulation (GDPR) became enforceable on May 25, 2018. The GDPR imposes new rules on companies, government agencies, non-profits, and other organizations that offer goods and services to people in the EU, or that collect and analyze the personal data of anyone residing in the EU, whether or not they are citizens. The GDPR applies to these organizations no matter where they are located. Given the GDPR's broad reach, Microsoft Online Services are designed to help you comply with the regulation regardless of where you are across the globe. Some important points:

Processor and controller roles. When you use Microsoft Online Services or Professional Services, you are the data controller and we are the data processor (except when you act as a processor of personal data, in which case we are the subprocessor and except when stated otherwise in the DPA Terms) for all personal data, customer data and professional services data. We will only process these data based on your documented instructions. The volume licensing agreement, including the DPA Terms, and the way in which you configure and use the service form your documented instructions. We are an independent data controller for our use of the data needed to perform the legitimate business operations incident to providing the Online Services and Professional Services.

How we demonstrate compliance with our data processor responsibilities: The International Standards Organization, through a multiyear deliberative process involving national standards bodies from the EU Member States and other countries, has developed a new standard that covers the management of Personally Identifiable Information. This new standard is known as the Personal Information Management System, or PIMS. Published in August 2019 as ISO 27701, Microsoft has already published guidance on how our controls align to ISO 27701 and plans to certify both Microsoft 365 and Azure against this standard because Microsoft believes that it provides a solid basis on which to evaluate Microsoft's handling of personal data and our adherence to contractual commitments. PIMS is designed to be used by both data controllers and processors to evaluate their compliance with the control system. It includes a section, Appendix D, that provides a rich mapping between PIMS and the ISO 27018 controls as well as GDPR. A copy of the full standard is available for purchase from the ISO website here. Due to copyright restrictions, we are unable to provide the text of the standard to you directly, but we have been advocating that ISO make the standard available publicly without charge.

How we assist you with your data controller responsibilities: Microsoft has developed the following materials to help you comply with GDPR:

- Accountability Readiness Checklists for Azure, Dynamics, Office 365 and Microsoft Professional Services outline the potential obligations you may have under the GDPR and point you to information that you can use to support your organizations' compliance.
- Data Subject Requests (DSRs) Guides under the GDPR and CCPA using Microsoft products and services can be found here.

- Breach notification details for Azure, Dynamics, Office 365 and Microsoft Professional Services can be found here.
- Information regarding Data Protection Impact Assessments (DPIAs) under the GDPR when using Microsoft products and services can be found here.

California Consumer Privacy Act (CCPA) assurances

The CCPA is a relatively new regulation regarding personal information collected by businesses when doing business in the state of California. Customers who need to comply with this law often ask whether Microsoft retains, uses or discloses their data for any purpose other than the purposes set out in the DPA Terms. The answer is a clear and resounding no. When you use Microsoft Online Services, you can rest assured that Microsoft never mines or uses your data for advertising, and Microsoft never sells your data.

Emerging regulations

Frequent updates to the laws and rules from the many regulatory bodies around the world create a challenge for organizations. Compliance personnel need assistance to help meet evolving requirements. Microsoft helps you meet compliance obligations under the shared responsibility model for public clouds by providing an extensive repository of resources that include tools, documentation, and guidance. An exemplary list of resources that can simplify your privacy burden include:

- Microsoft Compliance Score and Microsoft Compliance Manager are companion tools that provide insights into your organization's compliance posture and recommend actions that you can take to reduce compliance risks in Office 365 environments. Azure Security Center compliance dashboard provides similar insights and recommendations for Azure environments.
- Delta Lake on Azure Databricks is a compliance tool that helps you manage GDPR and CCPA data subject requests for your data lake.
- Azure Information Protection helps organizations classify and protect documents and emails by applying labels that can be applied automatically by administrators who define rules or manually by users.
- More solutions for managing information governance and preventing fraud can be found in Office 365 and Dynamics service-specific documentation.

We believe that all requests for your data should be directed to you.

If we receive a third-party request for your data, including from law enforcement, we will redirect that request to you unless required by law to comply.

- Microsoft does not give any government (including law enforcement or other government entities) direct or unfettered access to customer data.
- If any third party wants customer data, it needs to follow applicable legal process–meaning, it must serve us with a valid legal process for data or subscriber information or other non-customer data.
- For non-governmental requests, we require specific lawful consent of the account owner to release data and, for all requests, we provide notice to the account owner unless prohibited by law from doing so.
- Microsoft does not provide any government with platform encryption keys or provide governments with the ability to break customer enabled encryption.

How we respond to law enforcement demands

If a government wants customer data, it must follow applicable legal process.

- All legal demands for customer data must target specific accounts and identifiers.
- Microsoft's legal compliance team reviews all legal demands to ensure they are valid, rejects those that are not valid, and only provides specific data in response.
- If Microsoft is compelled by law to disclose customer data, you will be promptly notified and provided with a copy of the legal demand, unless Microsoft is legally prohibited from doing so.

Microsoft imposes carefully defined requirements on government and law enforcement legal demands for customer data. Such legal demands for customer data must comply with applicable laws. When governments or law enforcement agencies make a lawful request for customer data, Microsoft is committed to transparency and limits what it discloses.

Our transparency reports help you understand the numbers

Twice a year, we publish the number of legal demands for customer data that we receive from law enforcement agencies around the world. See Law Enforcement Requests Report. This report does not disclose the specifics of any particular demand, including the customer at issue. Twice a year, we

also publish data about the legal demands we receive from the U.S. government. See US National Security Orders Report.

- Overview of the legal work done at Microsoft to reform international agreements, participate in legal cases or reform laws to protect customer data.
- Details about our practices including Frequently Asked Questions addressing concerns customers have about government and law enforcement requests, including questions about the CLOUD Act.
- The Six Principles for international agreements governing law-enforcement access to data and a deep explanation of these principles.


Microsoft