Microsoft Professional Services And Support Data Protection

May 2018

MICROSOFT CORPORATION

Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • US

CONTENTS

Table of Contents

Introduction

Headlines around the world have many expressing concerns around the privacy and security of their data. Every day, you and many others rely on Microsoft's Professional Services organization to deliver technical support and consulting services. As part of this, you entrust Microsoft with your data, and rightly ask what we are doing to protect it. You want to know what our approach is, what independent verification there is of that trust, and if we will contractually commit to specifics on how we protect your data.

Maintaining security and privacy across a complex and global organization like Professional Services is particularly challenging. We are required to support more devices, platforms, and places than ever before. To do this, we balance the need for access to data to perform our mission against the reality that broader access makes security management more challenging.

The purpose of this document is to demonstrate how we address those challenges, and to provide a response to your questions regarding data protection controls and compliance in the Professional Services information governance environment.

About Microsoft's Professional Services Organization

Microsoft Professional Services is a global organization of more than 20,000 employees in more than 60 countries who strive to build enduring customer relationships by providing world class consulting services, commercial support, customer service, and contact center support for all Microsoft products and services. With more than 50 million customer contacts each year, Professional Services is often the first point of contact for Microsoft customers.

Professional Services also provides a vital function for Microsoft through its customer feedback systems, by which Professional Services is a customer advocate helping Microsoft evolve its products, programs, and services to address customer needs.

Professional Services provides both reactive support, responding to customer needs, and proactive support, reaching out to customers to assist with the configuration and optimization of their systems and to prevent problems and risks before they begin. Additionally, Professional Services provides a wide variety of consulting services including strategic advisory, migration services, IT services and other solutions.

To accomplish its mission, Professional Services necessarily collects or accesses support and consulting data through a variety of means from online self-help or web forms to assisted phone, email, and chat all the way to remote access of customer machines or on-site engagements. Data collection may include information about hardware, software, and other details related to an IT environment, contact or authentication information, chat session personalization, information about the condition of a computer and application during diagnostics, system and registry data about software installations and hardware configurations, and error-tracking files.

Our Approach to Data Protection

Professional Services is a complex, globally distributed organization and protecting support and consulting data is a core priority. Our strategy for addressing data protection in our IT systems includes defense-in-depth security, built-in privacy, transparency, and stringent compliance, actively managed by a group of discipline experts across business units and geographic regions.

Professional Services Information Protection and Governance Team (IPG)

The IPG team consists of experienced data protection professionals responsible for privacy and security of support and consulting data collected by Professional Services, managing risk, and ensuring compliance with legal, regulatory, and industry requirements, as well as internal policies and standards.

The team is made up of certified security, privacy, risk and compliance/audit professionals, and is organized into governance, risk, compliance, information security, privacy, and regulatory affairs units.

A few examples of IPG activities:

- Developing, implementing, and ensuring compliance with Microsoft and Professional Services security and privacy policies and related processes (for example, privacy and data classification standards)
- Identifying information governance related risks, implementing and monitoring mitigating controls, and resolving security & privacy incidents, including root cause analyses and overseeing remediation
- Developing and deploying data protection training and awareness
- Ensuring diagnostic tools, internal line of business applications, and systems are compliant with policies
- Managing and verifying supplier governance and compliance

IPG is supported by additional subject matter experts at Microsoft's corporate level, including within Microsoft's compliance and legal organization, the Corporate External and Legal Affairs (CELA) group. CELA is responsible for creating corporate policies and standards, coordinating cross-business requirements and responses on incidents and issues, and ensuring that Microsoft's strategy of embedding data protection into all products and services is executed. In addition, the CELA Regulatory Affairs Group is responsible for monitoring and reviewing data protection laws and regulations as well as industry developments around the world. They also provide legal guidance regarding our corporate policies and standards.

Data Protection Business Enablement Team

Professional Services also relies on the IPG Business Enablement team, a group of experts attached to business units in various geographic regions that assist in driving compliance within those business units. In an organization as complex and geographically distributed as Professional Services, an understanding of how our individual businesses operate allows our experts to provide tailored security and privacy solutions while ensuring compliance with Professional Services' standards and requirements.

Independent Verification and Compliance

Many customers ask to audit our facilities or systems or come to us with complex compliance requirements. Given the volume of customers and data that Professional Services handles in shared facilities, it is not practical to allow individual customer organizations to conduct audits on our systems.

To address this matter, Professional Services has operationalized data protection into a scalable, formalized, verifiable process that enables the organization to quickly adapt to security trends and industry-specific needs. Professional Services engages in regular risk assessments and develops and maintains a governance framework that meets the latest standards. For an additional level of governance and to enable deeper customer trust, Professional Services undergoes external audits and certification by trusted independent organizations. In addition to these internal reviews and external certifications, we add contractual guarantees so that customers have assurance their information is appropriately protected.

Professional Services has obtained independent verification, including ISO/IEC 27001 certification and ISO/IEC 27018 attestation. Professional Services is also compliant with the European Union General Data Protection Regulation (GDPR) and capable of transferring data outside of the European Union (EU) through EU Model Clauses and EU-US Privacy Shield (and Swiss-US Privacy Shield). In addition, Professional Services can sign a HIPAA Business Associate Agreement (BAA) with qualified healthcare customers. Professional Services maintains specialized offerings to satisfy the compliance requirements of public sector customers, including United States (US) federal and EU governments. We extend to you many of the controls implemented to meet these standards, regardless of whether you are subject to the respective laws or controls.

ISO 27001:2013 and ISO 27018:2014

The highly regarded ISO/IEC 27001 standard for information security management systems forms the foundation of our security and privacy approach for our Professional Services business. ISO/IEC 27001 is one of the most widely recognized certifications by international organizations and regulators and is one of the most valued by our customers.

In 2014, ISO adopted ISO/IEC 27018:2014, an addendum to ISO/IEC 27001, the first international code of practice for cloud privacy. Based on EU data protection laws, it gives specific guidance to cloud service providers acting as processors of personal data on assessing risks and implementing state-of-the-art privacy controls.
Due to the complexity of the Professional Services, we currently maintain several different ISO 27001 certifications for different parts of our business. One covers the Professional Services business management, consulting services and technical support teams. This certification demonstrates that the entire organization is compliant with ISO 27001 requirements, with the necessary procedures, training, and systems. Additional certificates cover the Microsoft Online Services that are leveraged by the Professional Services Organization and the data centers that store data provided to Professional Services.

Our independent auditor, the British Standards Institute (BSI) of America, verifies the compliance of the Professional Services organization to ISO 27001 requirements on an annual basis, and validates that Microsoft's support of in-scope enterprise cloud services have incorporated ISO/IEC 27018 controls for the protection of

personal data. At the same time, BSI reviews additional privacy controls we build into the service to better align it with comprehensive EU data protection regulations. We take this unique approach to help our European customers understand the protections we put in place and to help them satisfy the expectations of both European citizens and European regulators.

These certifications are available from BSI, linked to from the bottom of this report. The full scope of the audit and results of BSI's findings are included in its ISO 27001 audit reports, a copy of which is available to customers on request.

Microsoft Professional Services Data Protection Addendum (MPSDPA)

For Unified Support, Premier Support, and Microsoft Consulting Services customers, your agreement includes an enhanced set of contractual guarantees. This addendum, linked to below, describes Microsoft privacy and security practices as they pertain to support and consulting data processed by the Professional Services organization.

European Union Regulation

The General Data Protection Regulation (GDPR) is a European Union law that governs the processing of personal data. Professional Services includes GDPR language within the MPSDPA and provides extensive additional documentation in the Microsoft Trust Center (through the Microsoft Trust Portal) regarding GDPR compliance. In addition, to facilitate legal transfers of data outside the European Union, Microsoft incorporates the European Union Model Clauses (EUMC) into the MPSDPA for Commercial Support, and on request for Consulting Services.

HIPAA BAA

The Health Insurance Portability and Accountability Act (HIPAA) is a US law that requires HIPAA Covered Entities to meet certain privacy and security standards with respect to personal health information (PHI). To assist our customers utilizing the Professional Services organization in meeting their HIPAA compliance obligations, Microsoft will sign a Business Associate Agreement (BAA) with qualified HIPAA Covered Entities.

Public Sector Regulation

Professional Services has developed a set of specialized offerings to satisfy the compliance requirements of public sector customers, including those of US government customers and some EU governments. For US government customers, solutions are available that restrict access to US nationals, individuals with Position of Public Trust clearance, or, in some cases, geographically to the US. These options are also designed to work with public sector cloud offerings (i.e. FEDRAMP) from Microsoft Office 365, Dynamics 365, and Azure Services.

Built-in Security

Professional Services has a sophisticated control environment designed to drive compliance with Microsoft policies and to maintain appropriate security practices. An overview of key controls and the risks they mitigate is provided below.

24-Hour Monitored Physical Hardware

Support and consulting data is normally stored in Microsoft data centers, run by Microsoft's Azure Global Operations organization, and strategically located around the world. Our data centers are designed, built, and managed using a defense-in depth strategy, to protect services and data from harm by natural disaster or unauthorized access. Data center access is restricted 24 hours per day by job function so that only essential personnel have access to customer applications and services. Physical access control uses multiple authentication and security processes, including badges and smart cards, biometric scanners, on-site security officers, continuous video surveillance, and two-factor authentication. The data centers are monitored using motion sensors, video surveillance, and security breach alarms. In case of a natural disaster, security also includes seismically braced racks where required and automated fire prevention and extinguishing systems. For more on security in the Microsoft data centers that host Professional Services' data, please see the Microsoft Trust Center), linked to from the bottom of this report.

In some cases where Professional Services data requires in-depth analysis, it may also be stored either in a lab environment or on an engineer's laptop. Customer Support Labs use appropriate security based on risk level and location. Laptops are encrypted with BitLocker and adhere to Microsoft Security Policy. You may always inquire around specific security measures if your data is required to be stored at a separate facility.

Access Management

Stringent system access control mechanisms and processes limit access to those with a genuine business need, on a least privileged basis. For example, the Commercial Support case management system can only be accessed by individuals who are supporting customers, such as agents, support engineers, and their supervisors. User access reviews are conducted on an ongoing basis to verify that all users have a business need and have the appropriate level of access. This also ensures that the access of personnel who change roles, leave Microsoft, or haven't accessed systems for an extended period are appropriately revoked. Account password controls enforce complexity rules, periodic rotation, and suspension where periods of inactivity are detected.

Commercial Support personnel's normal procedure is to only use Microsoft-approved remote assistance tools to access customer managed environments. Use of these approved tools ensures that data is adequately protected when remotely accessing a customer's computer or network.

Authorized Use of Information

Professional Services has developed requirements and designed systems to prevent personnel who have authorized access to support and consulting data from using it for purposes beyond those identified for their

roles. Systems have limited export functionality and some employ field-level security (for example, inability to see data fields that are not relevant to an individual's role even though the individual has authorized access to the system). These controls also help prevent data from being read, copied, altered, or removed without authorization.

System Logging and Auditing

Professional Services takes a risk-based approach to logging and auditing of systems. A baseline set of log requirements is assessed and implemented during the system development process. Systems that present a moderate or high risk as assessed through sensitivity, volume, and other criteria have data access and alteration logged. Logs generated for each system enable the detection of security incidents if they have occurred or are in progress and provide investigators information needed to fully understand the events, activities, and circumstances around a security incident. Included in the information logged are the name of the individual accessing the data, what was accessed, and when it was accessed.

Human Resources Security

All Microsoft personnel with access to support and consulting data are responsible for ensuring compliance with data protection policies and standards, and are made aware of this during regular training, as described below. Personnel are also required to sign agreements committing them to confidentiality. Additionally, when appropriate, internal tools contain data protection notices, reminding personnel and data handlers of their responsibility regarding the sensitivity of data that the tool may contain.

Personnel who violate Microsoft's policies, including privacy and security policies, may be subject to disciplinary action. Where appropriate and permissible, background checks are completed on personnel who may have access to support and consulting data or who are in a role that could impact customer information.

Business Continuity for Microsoft Commercial Technical Support Organization

Microsoft recognizes that our products, services, and devices are used by customers in mission-critical environments. As a result, Microsoft has designed and implemented support capabilities to assist customers with questions and issues relating to the deployment and use of our products and services. Professional Services has a robust business continuity management (BCM) program intended to provide continued access to support and to protect and manage support data according to Enterprise guidelines.

Business Continuity Management Program

Commercial Support maintains one of the most mature business continuity management programs across the enterprise. Commercial Support Business Continuity plans align with the Microsoft's Enterprise Business Continuity Management program and policy to support continuous delivery of essential business services. Business Continuity plans to recover from minor incidents (for example, localized disruptions of business

components) to major disruptions (for example, fire, natural disasters, extended power failures, equipment, and/or telecommunications failure) are regularly updated and exercised.

Global Mission Control, a 24x7 geographically diverse team, leverages the business continuity plans to manage planned and unplanned interruptions globally for the support organization, including event response and crisis management.

High Availability

Commercial Support utilizes cloud-based call routing technologies which are designed to be highly available and route calls to the best available resource across the globe for quickest resolution. If any support location becomes unavailable calls are automatically routed to alternate locations ensuring seamless transition and continuity of support.

Multi-Channel Support

Within Commercial Support, solutions are delivered across multiple channels: online, self-help, community and assisted support for all products and services. This allows customers to choose their best support option and ensures support services are always on for customers when they need them and where they need them.

Data Recovery

Critical systems and infrastructure that store support data have stringent recovery requirements to minimize any data loss and are designed to protect customer information in compliance with Microsoft Enterprise security standards and requirements. Critical support infrastructure is hosted across geographically-diverse data centers with load balancing or automatic failover capability.

Business Continuity Training and Testing

All Commercial Support personnel assigned to coordinate and manage the development, implementation, maintenance, or communication for components of their respective business continuity program receive appropriate training based on their roles to be prepared in the event of a business continuity incident.

Critical infrastructure and systems, including any third-party components are regularly tested to establish and validate recovery capability. Full scale and functional Business Continuity exercises are conducted in production environments to review the recovery capability of key business processes. Results of such tests and exercises are periodically reported to Microsoft Senior leadership.

Information Governance & Compliance

Security and privacy practices rely on a set of underlying information governance and compliance policies, standards, and procedures. Following are some of the key safeguards that have been put in place to ensure ongoing compliance.

Information Security Policy

Professional Services adopts a layered approach to compliance, relying on policy for general principles, standards for specific requirements that must be followed, and operating procedures to describe day-to-day implementation. Professional Services maintains a control framework of over 150 controls to ensure compliance with policies and standards.

Professional Services adheres to the Microsoft company-wide Security Policy. Implementation of the principles in this Security Policy are driven by policies and standards that are specific to Professional Services and cover areas ranging from access control to data handling to privacy and business continuity. In addition, each team in Professional Services maintains operating procedures detailing how their business responsibly implements these requirements.

To ensure adherence to data protection policies and standards, Professional Services uses a process of monitoring that requires a regular cycle of evidence collection. Testing of required functionality occurs annually, semi-annually, quarterly, monthly, or, for software, at the time of each new release, depending on the level of risk associated with this particular privacy or security control.

Information Security Policies and standards have been approved by management and are regularly reviewed and communicated to personnel.

This multi-layered and continuous approach to monitoring data protection across environments helps to quickly diagnose and remedy problems that occur and helps support customers' need to respond quickly to shifting regulatory or industry requirements.

Data Classification and Protection

Professional Services implements a risk-based approach to data protection that weighs access to data and other protections against the sensitivity of each data classification. This allows for the business to while being sensitive to data that is critical, heavily regulated, or high value. The Data Classification, Protection, and Usage policies and standards defines requirements for classification of Professional Services data and specifies how each classification is to be handled.

It sets out classification categories for information based upon the sensitivity of the data and other requirements. Data protection and usage requirements, including:

- Transferring data
- Encryption

- Storage
- Data Usage and Handling
- Retention and Disposal
- Physical transport

System and Software Development

Systems and software tools used to provide services and support at Microsoft undergo the Security Development Lifecycle (SDL), a comprehensive security assurance review that informs every stage of design, development, and deployment of Microsoft software and services. SDL may include design requirements, analysis of attack surface, and threat modeling. SDL helps Microsoft predict, identify, and mitigate vulnerabilities and threats from before a service is launched through its entire production life cycle. Microsoft continuously updates the SDL using the latest data and best practices to help ensure that systems and software associated with Professional Services are designed to be highly secure from day one.

Privacy Compliance

This section describes some of the key steps taken to ensure privacy compliance of data collected while providing professional services.

Notice and Transparency

Although many companies cite privacy and security concerns as major obstacles to choosing a support provider, information on the privacy and security practices of many providers is either difficult to find or indecipherable to all but the most astute IT professionals.

To help you find answers to your privacy and security questions about Professional Services, we strive to be as transparent as possible about our data protection policies and procedures. The Trust Center Professional Services section, linked to below, explains, in plain language, exactly how we handle and use data gathered in customers' interactions with Professional Services. You can find details about our commitments in key privacy areas, including data use limits, geographic boundaries, third parties, security, audits, and certifications and regulatory compliance in the Trust Center.

As a continuously evolving and improving service organization, the Trust Center serves as a living resource that customers can use to stay abreast of the most current and accurate information available about Professional Services' privacy and security practices.

Data Protection Training and Awareness

Professional Services maintains a comprehensive training and awareness program. All personnel are trained on privacy and security policies and processes, including updates. Training and awareness are delivered through multiple media, including live training, online, email, printed publications, and video training. Ongoing continual

awareness reinforces training through periodic email communications, posters, video displays, in-person meetings, and other means.

Data Collection and Usage

Professional Services collects data from customers to provide support and proactive guidance on preventing future support issues, and to deliver services that may help develop, onboard, deploy, run, improve or otherwise support Microsoft technology. Support and consulting data collected for these purposes will at times include customer-generated information containing their intellectual property, or the customer's own content in documents, emails, spreadsheets, websites or other confidential data. Examples include end-user personal data and emails, SharePoint data, financial information or cost model data. Professional Services protects this data in accordance with legal and regulatory requirements, certification standards, and contractual agreements.
Data provided by customers to Professional Services for non-technical support purposes, such as billing or subscription management, is used and protected in accordance with the Microsoft Privacy Statement. This may include, for example, customer contact, billing, or other account information.

Professional Services may collect this information in the following ways, among others:

- Over the phone (for example, when a customer calls, they may provide commercial support with information such as name, phone number, email address, and a description of the support issue)
- By accessing customer systems remotely with customer permission (for example, remote access via a tool to view server configurations over an encrypted channel to resolve support issues)
- By receipt of data via a secure file transfer system (for example, if support issues are not resolved by remote access, resolution may require that the customer upload data via the encrypted tool)

Data Transfers

Support and consulting data that Microsoft processes on a customer's behalf may be transferred to, stored, and processed in the US or any other country in which Microsoft maintains facilities. We do this to provide the best experience possible. In technical support, this allows us to maintain centralized management of data and geographically-distributed 24/7 support through a series of regionalized contact centers. In consulting services, this allows us to centralize consulting functions where it makes sense and always leverage a worldwide network of the highest quality expertise possible. When calling for remote support, customers can always ask where the agent or support engineer is located. The customer may also request to speak to personnel in their region. Microsoft will accommodate these requests to the extent possible based on time of day and urgency of the support request.

For customers in the EU, Microsoft offers customers EU Model Clauses, referred to as Standard Contractual Clauses, that make specific privacy guarantees allowing transfer of personal data. This ensures that Microsoft customers' data can legally be moved from the European Union to the rest of the world.

Data transfers are conducted with appropriate security safeguards. For example, customer data sent externally to Microsoft is encrypted. This includes data transferred from customers via our support software and tools.

Third Party Management

Microsoft relies on subcontractors to provide additional expertise during complex consulting solutions, as staff augmentation, and to ensure an optimal and round-the-clock support experience for our customers, no matter where they are located.

Subcontractors that work in facilities or on equipment controlled by Microsoft must follow our data protection policies and standards. All other subcontractors must follow data protection policies and standards equivalent to our own. Microsoft's agreements with its subcontractors have a variety of clauses designed to ensure the safeguarding of customer information, and we regularly monitor their compliance.

You may find more information regarding Microsoft's use of third parties on the Trust Center. A current list of subcontractors used in Professional Services is also available on the Trust Center.

Law Enforcement

Microsoft may occasionally receive law enforcement requests to provide support and consulting data. Microsoft does not disclose support and consulting data to law enforcement unless required by law. Should law enforcement contact Microsoft with a demand for support and consulting data, we will attempt to redirect the law enforcement agency request to the customer. As part of this effort, Microsoft may provide customer's basic contact information to the agency. If compelled to disclose support and consulting data to law enforcement, Microsoft will use commercially reasonable efforts to notify customer in advance of a disclosure unless legally prohibited.

Incident Response

Microsoft takes every security incident very seriously. Professional Services has developed a robust process to facilitate a coordinated response to incidents that may occur. Upon becoming aware of a security incident, we use this security incident response process, including forensic investigation, to track exactly what happened, which data was accessed, and by whom. We follow industry best practices at each step of the incident management process: identification/triage, containment, investigation, mitigation/eradication, notification, lessons learned, and communication. Our contractual obligations in the Microsoft Professional Services Data Protection Addendum require Microsoft to notify customers promptly in the event of a breach affecting their data.

Conclusion

Microsoft Professional Services are committed to ensuring and maintaining the security and privacy of support and consulting data entrusted to us. To deliver on this commitment, Professional Services maintains a robust control environment based on legal and industry standards and best practices. To prove this, Microsoft contractually commits to specifics of its data protection approach, and regularly undergoes independent audits. Microsoft's transparent approach to data protection means that additional information about the Professional Services data protection program is updated regularly on the Trust Center. When you choose Professional Services, you get a partner that truly understands your data protection needs and is trusted by companies of all sizes across nearly every industry and geography.

Additional Information

For additional information see:

- Professional Services portal on the Microsoft Trust Center: https://www.microsoft.com/en-us/trustcenter/professional-services
- Microsoft Trust Center: https://www.microsoft.com/en-us/TrustCenter
- BSI ISO/IEC 27001:2013 Certification: http://www.bsigroup.com/en-US/Our-services/Management-systemcertification/Certificate-and-Client-Directory-Search/Certificate-Client-Directory-Search-Results/?searchkey=company%3dmicrosoft%2bcorporation&licencenumber=IS 601002
- Microsoft Professional Services Data Protection Addendum: http://aka.ms/professionalservicesDPA.