Microsoft

Microsoft Managed Desktop data storage, usage, and security practices

This document provides information on data storage, usage, and security practices used by Microsoft Managed Desktop as of January 27, 2020.

Data usage of Microsoft Managed Desktop

These are the sources and use cases for data that Microsoft Managed Desktop is using.

Data sources and use	Use with Microsoft Managed Desktop
Windows diagnostic data	Used to determine the patch and update status of managed devices as well as to provide and improve Microsoft Managed Desktop's IT-as-a-Service (ITaaS) offering.
Intune data	Used in reports created for tenant admins, which are available in the Microsoft Managed Desktop Admin Portal.
Azure Active Directory data	Used in reports created for tenant admins, which are available in the Microsoft Managed Desktop Admin Portal.
Admin contact data	Used by Microsoft Managed Desktop to communicate with the tenant administrators.

Windows diagnostic data

Microsoft Managed Desktop process diagnostic data from Windows to provide its services to managed Microsoft Managed Desktop devices. Since the status information required by Microsoft Managed Desktop for providing it's IT-as-a-Service (ITaaS) is not already contained in the Basic Windows diagnostic data level, Microsoft Managed Desktop devices need to be set to the Enhanced level (the Enhanced diagnostic data level includes the data provided by the Basic data level). Microsoft Managed Desktop processes a subset of the Windows 10 Enhanced diagnostic data set. For more information about the Windows 10 Enhanced diagnostic data level, see Windows 10 diagnostic data events and fields collected through the limit enhanced diagnostic data policy.

Windows 10 Enhanced diagnostic data includes limited crash dump data used to improve the product. When a crash dump is needed as part of Windows Error Reporting, usually a triage dump – a sanitized version of a mini-dump with personal data removed – is generated and uploaded to Microsoft. For more information about Windows Error Reporting and crash dump files, see About WER and Analyze crash dump files by using WinDbg.

Microsoft Managed Desktop does not process these types of data normally included in the Enhanced diagnostic data level:

- Events about applications that are pre-installed with Windows such as Photos and Mail
- Device-specific events for devices such as Surface Hub and Microsoft HoloLens

Entities processed by Microsoft Managed Desktop

Microsoft Managed Desktop processes these entities to provide the service:

- Device data
- Device security settings
- Device operating system and hardware
- Aggregated information about device health
- Device diagnostic information
- Tenant data
- Azure Active Directory resources
- Policy and configuration data
- Windows diagnostic data
- Product and service usage data

Data storage

Microsoft Managed Desktop

Once in the service, Microsoft Managed Desktop stores data internally in U.S.- based Microsoft datacenters.

Microsoft Azure Active Directory

Identity data used by Microsoft Managed Desktop is stored by Azure Active Directory in a geographical location based on the address provided by the organization when subscribing for a Microsoft online service such as Office 365 or Azure. See Microsoft Azure — Where is my customer data? for a map showing the datacenters for Azure Active Directory.

For further information about the regions Azure uses for data storage, see Azure Active Directory – Where is your data located.

Microsoft Intune

Intune data can be stored in a few different regions, such as Europe North (Ireland) and Europe West (Netherlands). Your IT administrator creates a tenant account and chooses the country where data will be stored when they initially enroll in Intune services. For a list of datacenter locations used by Intune, see Microsoft Intune — Where is my customer data?. For more information about data storage and use by Intune, see Data collection in Intune.

Windows 10

As stated in the Microsoft Privacy Statement, "personal data collected by Microsoft may be stored and processed in your region, in the United States, and in any other country where Microsoft or its affiliates, subsidiaries, or service providers operate facilities. [...] Typically, the primary storage location is in the customer's region or in the United States, often with a backup to a datacenter in another region. The storage location(s) are chosen in order to operate efficiently, to improve performance, and to create redundancies in order to protect the data in the event of an outage or other problem. We take steps to ensure that the data we collect under this privacy statement is processed according to the provisions of this statement and the requirements of applicable law wherever the data is located."

For further information about the diagnostic data collection of Windows 10, see the "Where we store and process personal data" section of the Microsoft Privacy Statement.

Data access protection

Direct access to Microsoft Managed Desktop's internal data stores is restricted in several ways:

- Device data
    - It requires Engineering Lead level approval.
    - It is both audited and time limited.
    - It requires the use of a highly secured and restricted workstation.
    - All data is encrypted while it is stored.
    - There is no standing access.
    - Access to Microsoft Managed Desktop's internal management portal requires a highly secured and restricted workstation.

Security measures used by Microsoft Managed Desktop

Domain	Practices	
Security Ownership	Microsoft has appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures.	Azure, which Microsoft Managed Desktop uses as a compliance foundation and for compliance attestations, has assigned an Information Security Officer. In addition to that, Microsoft Managed Desktop has a dedicated security engineering team.
Security Roles and Responsibilities	Microsoft personnel with access to Customer Data are subject to confidentiality obligations.	Confidentiality obligations are covered by the Microsoft employment contract that all Microsoft employees have to sign.
Risk Management Program	Microsoft performed a risk assessment before processing the Customer Data or launching the Online Services service. Microsoft retains its security documents pursuant to its retention requirements after they are no longer in effect.	Microsoft Managed Desktop has a risk management program that also assesses the risks before processing personal data. The respective risk- and security-related documentation is retained as history documents.
Asset Inventory	Microsoft maintains an inventory of all media on which Customer Data is stored. Access to the inventories of such media is restricted to Microsoft personnel authorized in writing to have such access.	Being a Microsoft cloud service, Microsoft Managed Desktop uses Microsoft cloud storage such as relational databases and Microsoft Big Data platforms. Microsoft Managed Desktop maintains an inventory of the cloud services storage on which Customer Data is stored. The access to that inventory of cloud storage used is restricted to authorized Microsoft Managed Desktop personnel.
Asset Handling	Microsoft classifies Customer Data to help identify it and to allow for access to it to be appropriately restricted. Microsoft imposes restrictions on printing Customer Data and has procedures for disposing of printed materials that contain Customer Data. Microsoft personnel must obtain Microsoft authorization prior to storing Customer Data on portable devices, remotely accessing Customer Data, or processing Customer Data outside Microsoft's facilities.	Microsoft Managed Desktop classifies Customer Data and restricts access to it with several layers of protections. Policies disallowing printing of customer data are also in place as part of Azure's Standard Operating Procedures. Authorization is required for Microsoft Managed Desktop prior to remotely accessing Customer Data and processing Customer Data outside of Microsoft's facilities.

Domain	Practices	
Security Training	Microsoft informs its personnel about relevant security procedures and their respective roles. Microsoft also informs its personnel of possible consequences of breaching the security rules and procedures. Microsoft will only use anonymous data in training.	Corporate-wide Microsoft security training requirements, such training at least annually.
Physical Access to Facilities	Microsoft limits access to facilities where information systems that process Customer Data are located to identified authorized individuals.	Physical access restrictions are in place for Microsoft Managed Desktop to limit the access to information systems where customer data is processed.
Physical Access to Components	Microsoft maintains records of the incoming and outgoing media containing Customer Data, including the kind of media, the authorized sender/recipients, date and time, the number of media and the types of Customer Data they contain.	Physical access to media containing customer data is not applicable for Microsoft Managed Desktop, since as a Microsoft cloud service, Microsoft Managed Desktop uses Microsoft cloud storage such as relational databases and Microsoft's big data platforms for storing information. Physical access to media containing customer data is inherited by the organization operating the Azure data centers that Microsoft Managed Desktop is using.
Protection from Disruptions	Microsoft uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference.	Microsoft has several mechanisms in place, including Business Continuity and Disaster Recovery (BCDR), as protection against loss of data due to power supply failure or line interference.
Component Disposal	Microsoft uses industry standard processes to delete Customer Data when it is no longer needed.	Microsoft Managed Desktop uses the corporate provisions Microsoft has created for that purpose.
Operational Policy	Microsoft maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Customer Data.	Microsoft Managed Desktop maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Customer Data.

Domain	Practices	
Data Recovery Procedures	On an ongoing basis, but in no case less frequently than once a week (unless no Customer Data has been updated during that period), Microsoft maintains multiple copies of Customer Data from which Customer Data can be recovered.	As a Microsoft cloud service using Azure, which has proper provisions in place for addressing data recovery procedures, this is covered by Azure and the team that operate the Azure data centers.
	Microsoft stores copies of Customer Data and data recovery procedures in a different place from where the primary computer equipment processing the Customer Data is located.	Being a Microsoft cloud service using Azure, which has proper provisions in place for addressing data recovery procedures, this is covered by Azure and the team who operates the Azure data centers.
	Microsoft has specific procedures in place governing access to copies of Customer Data.	Microsoft Managed Desktop uses proper access restrictions, such as role-based access and "just-in-time" access, to govern the access to copies of Customer Data.
	Microsoft reviews data recovery procedures at least every six months, except for data recovery procedures for Azure Government Services, which are reviewed every twelve months.	As part of our business continuity and disaster recovery (BCDR) obligations, Microsoft Managed Desktop reviews data recovery procedures at least every six months.
	Microsoft logs data restoration efforts, including the person responsible, the description of the restored data and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process.	As part of its BCDR operation processes, Microsoft Managed Desktop logs the data restoration efforts.

Domain	Practices	
Malicious Software	Microsoft has anti-malware controls to help avoid malicious software gaining unauthorized access to Customer Data, including malicious software originating from public networks.	As a Microsoft cloud service using Azure, Microsoft Managed Desktop has various anti-malware controls in place helping to avoid malicious software gaining unauthorized access to Customer Data.
Data Beyond Boundaries	Microsoft encrypts, or enables Customer to encrypt, Customer Data that is transmitted over public networks.	As a Microsoft cloud service using Azure, Microsoft Managed Desktop encrypts Customer Data that is transmitted over public networks for the operations it controls. Microsoft enables customers to transmit Customer Data over public networks in an encrypted fashion, for example by using https transmissions.
	Microsoft restricts access to Customer Data in media leaving its facilities.	As a Microsoft cloud service, Microsoft Managed Desktop uses Microsoft cloud storage such as relational databases and Microsoft big data platforms for storing information. Physical access to media containing customer data is inherited by the team operating the Azure data centers that Microsoft Managed Desktop uses. Microsoft restricts access to Customer Data in media leaving its facilities, for example by using encrypted media.
Event Logging	Microsoft logs, or enables Customer to log, access and use of information systems containing Customer Data, registering the access ID, time, authorization granted or denied, and relevant activity.	Microsoft Managed Desktop logs access and use of information systems containing Customer Data and keeps track for example of access ID and time as well as status information such as authorization granted or denied.
Access Policy	Microsoft maintains a record of security privileges of individuals having access to Customer Data.	Microsoft Managed Desktop logs this information for maintaining a record of security privileges of individuals having access to Customer Data.

Domain	Practices	
Access Authorization	Microsoft maintains and updates a record of personnel authorized to access Microsoft systems that contain Customer Data.	Microsoft Managed Desktop maintains and updates a record of personnel authorized to access Microsoft systems that contain Customer Data, for example by using role-based access models.
	Microsoft deactivates authentication credentials that have not been used for a period of time not to exceed six months.	By using role-based access models that have to be reviewed regularly, Microsoft Managed Desktop assures that credentials that haven't been used for six months are getting deactivated.
	Microsoft identifies those personnel who may grant, alter or cancel authorized access to data and resources.	Microsoft Managed Desktop has processes in place, and assigned owners to them, for granting, altering, and cancelling access authorization to data and resources.
	Microsoft ensures that where more than one individual has access to systems containing Customer Data, the individuals have separate identifiers/logins.	Microsoft Managed Desktop ensures that individuals are using separate identifiers or sign-in credentials for systems containing Customer Data to that more than one individual can access.
Least Privilege	Technical support personnel are only permitted to have access to Customer Data when needed.	Microsoft Managed Desktop uses common Microsoft and industry security practices to ensure that technical support personnel have access to Customer Data only when needed.
	Microsoft restricts access to Customer Data to only those individuals who require such access to perform their job function.	Microsoft Managed Desktop has implemented various technical measures, including role-based access mechanisms, "just-in-time" access restrictions, and the use of highly secured workstations for restricting access to Customer Data.
Integrity and Confidentiality	Microsoft instructs Microsoft personnel to disable administrative sessions when leaving premises Microsoft controls or when computers are otherwise left unattended.	Following Microsoft security policies and practices, Microsoft Managed Desktop personnel are instructed to lock access their administrative sessions when leaving premises Microsoft controls or when they leave their computers unattended.
	Microsoft stores passwords in a way that makes them unintelligible while they are in force.	Microsoft Managed Desktop uses the highly secure Azure KeyVault solution for storing tenant-related passwords.

Domain	Practices	
Authentication	Microsoft uses industry standard practices to identify and authenticate users who attempt to access information systems.	These are common Microsoft security policies and practices that Microsoft Managed Desktop personnel must follow as well.
	Where authentication mechanisms are based on passwords, Microsoft requires that the passwords are renewed regularly.	These are common Microsoft security policies and practices that Microsoft Managed Desktop personnel must follow as well.
	Where authentication mechanisms are based on passwords, Microsoft requires the password to be at least eight characters long.	These are common Microsoft security policies and practices that Microsoft Managed Desktop personnel must follow as well.
	Microsoft ensures that de-activated or expired identifiers are not granted to other individuals.	These are common Microsoft security policies and practices that Microsoft Managed Desktop personnel must follow as well.
	Microsoft monitors, or enables Customer to monitor, repeated attempts to gain access to the information system using an invalid password.	Microsoft Managed Desktop monitors repeated attempts for gaining access to the information system using an invalid password, for example by examining Azure Active Directory logs.
	Microsoft maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed.	These are common Microsoft security policies and practices that Microsoft Managed Desktop personnel must follow as well.
	Microsoft uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage.	These are common Microsoft security policies and practices that Microsoft Managed Desktop personnel must follow as well. In addition, Microsoft Managed Desktop uses the highly secure Azure KeyVault solution for storing tenant-related passwords.

Domain	Practices	
Network Design	Microsoft has controls to avoid individuals assuming access rights they have not been assigned to gain access to Customer Data they are not authorized to access.	These are common Microsoft security policies and practices that Microsoft Managed Desktop personnel must follow as well. Microsoft Managed Desktop's security mechanisms are based on identities and role-based access controls.
Incident Response Process	Microsoft maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data.	This is a central Microsoft policy and standard Microsoft operation.
	For each security breach that is a Security Incident, notification by Microsoft (as described in the "Security Incident Notification" section above) will be made without undue delay and, in any event, within 72 hours.	This is handled centrally by a dedicated team. Microsoft has provisions for handling security breaches properly, including notifying customers.
	Microsoft tracks, or enables Customer to track, disclosures of Customer Data, including what data has been disclosed, to whom, and at what time.	This is a central Microsoft policy and standard Microsoft operation.
Service Monitoring	Microsoft security personnel verify logs at least every six months to propose remediation efforts if necessary.	Microsoft Managed Desktop reviews for example access logs and alerts about unauthorized accesses regularly and propose remediation efforts to address it. We force mandatory log reviews for role-based access mechanisms.