HP DaaS Proactive Management with HP TechPulse

Data Management FAQ

This document answers the most commonly asked questions related to HP Device as a Service (HP DaaS) Proactive Management with HP TechPulse **(***henceforth Proactive Management***),** data collection, transmission, storage, retention and disposal of data.

Contents

HP DaaS Proactive Management with HP TechPulse - Data Management FAQ

Cloud Technology/Data Centers

Q: What cloud technology and data centers are leveraged by HP DaaS Proactive Management?

A: HP DaaS Proactive Management is hosted on Amazon Web Services (AWS).

Proactive Management maintains data centers in Oregon, United States (AWS-OR) and Frankfurt, Germany (AWS-DE). Data for customers located in European countries can be hosted in the German data center. Data for customers in all other countries can be hosted in the U.S data center. All data within a single customer "tenant" is hosted in a single data center, although customers who wish to have separate tenants in different data centers to host data for different business units may request this option.

To learn more about AWS, visit https://aws.amazon.com.

Q: What are the roles of each data center with respect to tasks and customers?

A: The United States and German data centers can be used to differentiate customers from different regions and act as regional data centers. European-based customers may prefer to use the German regional data center, while customers from all other countries may prefer to use the U.S. regional data center. Having the two data centers, allows DaaS Proactive Management to localize personal data within each of the regions.

Data analytics for Proactive Management is performed in the United States Analytics data center (Oregon, United States (AWS-OR)). For data protection purposes, all personal data is de-identified prior to transmission and storage in the U.S. Analytics data center.

Identity management for Proactive Management is performed in two geographically dispersed locations on the Amazon Web Services within United States. Proactive Management uses a unified identity management ecosystem for all HP customers across all HP applications. This unified identity management primarily stores all the core data needed for an identity to authenticate (for e.g., first name, last name, email address, country of residence, mailing address, phone number password, and locale including credential recovery methods if needed). The exact location of these data centers cannot be disclosed due to security reasons.

Q: How does the data flow between the device and various HP DaaS Proactive Management components?

A: Data flow follows this process:

1. After an account is created, the Proactive Management customer enrolls in the cloud-based HP DaaS portal, which is hosted in U.S. and German regional data centers.
2. Proactive Management software is then pushed to customer's devices to enroll individual devices to be managed by Proactive Management from either the U.S. or German regional data center.
3. The cloud-based HP DaaS portal and the Proactive Management software on the devices capture and send data to the U.S. and German regional data centers.
4. Personal data maintained in the U.S. and German data center is de-identified before transmission to the U.S. Analytics data center where it will be leveraged for analytics purposes.
5. Proactive Management uses the cloud-based HP DaaS portal to provide its functionality—device management as well as analytical services (such as device health monitors, actionable reports, incidents, and alerts) by combining de-identified analytic data from the U.S. Analytics data center with personal data and information from the regional data centers.

Data Collection

Q: What data does Proactive Management collect and how is it used?

A: The "types" of data collected by Proactive Management are either provided by the customer directly or collected automatically from the cloud-based HP DaaS portal and the Proactive Management software on the devices.

Proactive Management collects the following data to execute contract services:

Purpose of Data Collection	Data Collected	Description of data collected
Account management	Account data	Information such as how a customer purchases or signs up for Proactive Management, support history with respect to incidents generated by Proactive Management, and anything else relating to the Proactive Management account to perform transaction services like account management.
Ensure Proactive Management software and services works properly	Application data	Proactive Management software's version, installation status, data sharing choices and update details.
Account setup, identity management and entitlement validation	Contact data	Personal and/or business contact data including first name, last name, mailing address, telephone number, fax number, email address and other similar contact information for Proactive Management account setup and validation, services entitlement and e-mail notifications around incidents and services.
Deliver proactive IT service maintenance and management, and customer-centric reports/dashboards	Device data	Basic hardware information related to device: computer, operating system, amount of memory, region, language, time zone, model number, initial start date, age of device, device manufacture date, browser version, computer manufacturer, warranty status, unique device identifiers and additional technical information that varies by product.
		Hardware components such as battery, disk, BIOS, HP SureStart, display and graphics, plug and play devices and drivers, driver errors and driver crashes, memory, real-time clock, processor, system slots, environment variables, thermals, operating system, network interface, operating system and third-party patches, anti-virus and firewall status and applications, windows device security profile, and device management profiles and their status.
		Software applications installed on devices. **Note:** We do not scan or collect the content of any file or information that might be displayed by an application.
		Performance data: Battery, disk, CPU, memory and thermal utilization.
		Software application utilization with respect to frequency and time of usage, and impact of software utilization on hardware performance data (battery, disk, CPU, memory and thermal usage).
		Continued
		Network utilization: network transmission rates from the device.

Continued

Purpose of Data Collection	Data Collected	Description of data collected
Deliver proactive service maintenance and management of devices by pinpointing the location of a missing device	Location data	Geolocation data to enable location-based services. This feature is turned off by default for all customers and an option is provided for customers to enable or disable location-based services in H Proactive Management.
Authentication and authorization of user access to Proactive Management accounts and services	Security credentials	User passwords, password hints, and similar security information required for authentication to authorize users for access to HP Proactive Management accounts and services.

Q: What types of data is not collected by Proactive Management?

A: Proactive Management does not collect the following types of data:

- Demographic information (with the exception of country or language preferences)
- Financial account information, credit or debit card numbers, credit records, or payment data
- Social media or web browsing information
- Government-issued identifier such as social security, social insurance number, or Government ID
- Health information
- Sensitive data such as ethnic origin, political beliefs, trade union membership, health data, sexual orientation, and genetic data

Security

Q: What security measures are used by Proactive Management to protect personal data?

A: When capturing, transmitting and storing data, Proactive Management uses a variety of security technologies and procedures to help protect your personal data from unauthorized access, use, or disclosure. This includes:

- Data stored in the U.S. and German regional data centers:
  - The databases that contain personal data, located in U.S. and German regional data centers are encrypted.
  - Contact data (i.e., personal and/or business contact data including a customer and/or user's first name, last name, mailing address, telephone number, fax number, email address and other similar contact information for HP DaaS accounts) are stored in clear text in both the U.S. and German regional data centers.
  - Location data (i.e., real-time geolocation of the device captured by Proactive Management) is encrypted using the Proactive Management application level encryption and SHA256 hashing.
- Data stored in the U.S. Analytics data center:
  - Device, Application and Location data is de-identified and cannot be tied to an individual prior to being transmitted and stored in the U.S. Analytics data center.
  - The databases that contain data, located in U.S. Analytics data center is encrypted.
- Data stored in the U.S. Identity Management data center:
  - The databases that contain personal data, located in U.S. Identity Management data centers are encrypted.
  - Contact data (i.e., personal and/or business contact data including a customer and/or user's first name, last name, mailing address, telephone number, fax number, email address and other similar contact information for HP DaaS accounts) are stored in clear text in the U.S. Identity Management data centers.
  - Security credentials data (like HP DaaS account passwords) are not stored in clear text.

Q: What are the threat intelligence modelling techniques performed on Proactive Management?

A: Two different threat intelligence modeling techniques are performed on Proactive Management:

- Penetration Testing Execution Standard
- Open Web Application Security Project (OWASP)

  Proactive Management undergoes these tests for all new functionality being released and periodically for all minor enhancements to existing functionality.

Q. What are the processes and procedures to ensure physical and environment security?

A: Proactive Management subcontracts to Amazon Web Services for its data centers.Amazon Web Services then takes care of physical access protection.

The Amazon Web Services data centers are Tier 3+ as per AWS documentation https://aws.amazon.com/compliance/uptimeinstitute/.

- The Amazon Web Services compliance and certifications can be found at https://aws.amazon.com/compliance/
- Amazon Web Services takes care of protection against external and environmental threats (fire, flood, earthquakes etc)

Proactive Management uses tools from Amazon Web Services (for e.g., Cloud Watch) to monitor the performance of Amazon Web Services.

Data Transmission and Storage

Q: What data types are transmitted and stored by Proactive Management in the different data centers?

A: The following data types are transmitted and stored in the different data centers:

Data Category	U.S. Regional Data Center[1]	German Regional Data Center[2]	U.S. Analytics Data Center[3]	U.S. Identity Management Data Center[3]
Account data	Yes	Yes	No	No
Application data	Yes	Yes	Yes	No
Contact data	Yes	Yes	No	Yes
Device data	Yes	Yes	Yes	No
Location data	Yes	Yes	Yes	No
Security credentials data	No	No	No	Yes

[1] For non-European-based customers
[2] For European-based customers
[3] For all customers

Q: What data can a customer opt-out from sharing with Proactive Management?

A: The following table provides opt-out information:

Data Category	Opt-Out	Additional comments
Account data	No	
Application data	No	
Contact data	No	A customer's first name, last name, e-mail, address, phone number and country information are mandatory information for a customer to provide.
Device data	No See two exceptions in additional comments.	Two options are available for opting out of data collection: 1. Anti-virus and firewall status and applications 2. Software applications installed on devices
Location data	Yes	
Security Credentials data	No	

Q: What are the sources and methodology of data capture and frequency of data transmission by HP DaaS Proactive Management?

A: The sources and methodology of data capture and frequency of data transmission include:

Data Category	Source	Methodology	Transmission Frequency
Account data	Cloud-based HP DaaS portal	The data is provided by customer, to be entered either by an HP DaaS Service Expert or directly by the customer in cloud-based HP DaaS portal.	In real-time, based on changes to account data.
Application data	Cloud-based HP DaaS portal and HP DaaS Proactive Management software on the device	Automatic	Every 15 minutes, based on changes to application data.
Contact data	Cloud-based HP DaaS portal	The data is provided by customer, to be entered either by an HP DaaS Service Expert or directly by the customer in cloud-based HP DaaS portal.	In real-time, based on changes to contact data
Device data	Proactive Management software	Automatic	• Device data for analytics is transmitted once a day. • Device data for setting and monitoring device. management profiles and their status is transmitted either in real-time or once a day based on changes to device data.
Location data	Real-time geolocation of the device is captured by Proactive Management software	Automatic	In real-time or once every 12 hours, based on changes to geo-location data.
Security Credentials data	Cloud-based HP DaaS portal	The data is entered by the customer in the cloud-based HP DaaS portal.	In real-time, based on changes to security credentials data.

Q: What are the typical network transmission rates for data transferred from the device to the Proactive Management?

A: After the initial installation of the Proactive Management software on the device, the software:

- Does a periodic check for any new updates available in the cloud-based Proactive Management every four to twenty-four hours and does a self-update to any new version.
- Typically updates itself for any critical issues and security related issues on a frequent weekly basis. All major enhancements are done twice a year.

Typical network download rates for downloading the Proactive Management software to the device is 100 MB per device.

The Proactive Management software on the device sends application, device and location data to the U.S. and German regional data centers and the U.S. Analytics data center. The Proactive Management software sends data only if there is a change in any of the data attributes between current and previous time-period. This approach allows Proactive Management software to minimize the network packet size being transmitted from the device to the U.S. and German regional data centers and the U.S. Analytics data center. Typical network transmission upload rates per device on a given day are between 1-3 MB.

Q: What location data is captured, transmitted and stored by HP DaaS Proactive Management?

A: Customer address data

- A Proactive Management customer, using the cloud-based HP DaaS portal, can enter their own address information. for example: country, city, postal code, street address, etc.
- This information is entered manually by the customer.
- This information is then transmitted to and stored in the U.S. or German regional data centers and U.S.Identity Management data centers only.

Operating system country data

- The operating system locale of the devices enrolled in Proactive Management.
- This is automatically captured from the device using Proactive Management software on the device.
- This information is then transmitted to and stored in U.S. or German Regional data centers and U.S. Analytics data center.
- Personal data associated with the operating system country to be leveraged for analytics is de-identified before being transmitted and stored in the U.S. Analytics data center.

Device country data

- The country information of the devices enrolled in Proactive Management.
- This is automatically captured based on the current location of the device using Proactive Management software on the device.
- This information is transmitted to and stored in U.S. or German Regional data centers and U.S. Analytics data center.
- Personal data associated with the device country data to be leveraged for analytics is de-identified before being transmitted and stored in the U.S. Analytics data center.

Real-time device location data

- The real-time geolocation location of the device (for example: the latitude and longitude of the device)
- This data is captured only if a Proactive Manager customer enables location-based services for their devices from the cloud-based HP DaaS portal .
- This data is captured from the device using Proactive Management software on the device.
- The location-based services to track geolocation of devices by Proactive Management is turned off by default for all customers. An option is provided for customers to enable or disable location-based services in Proactive Management. Even when location-based services are turned on, Proactive Management does not allow for the collection of device location data for any devices classified as employee-owned or personal devices.
- This data is transmitted to and stored in U.S. or German regional data centers. Personal data associated with real-time device location data (i.e., real-time geolocation of the device captured by Proactive Management to be leveraged for analytics) is de-identified before being transmitted and stored in the U.S. Analytics data center.

Asset tracking location data

- Proactive Management allows customers to enter the location address of an asset using the Proactive Management service. This is not the real-time device location data, but rather a label to identify a physical location of the asset (for example, Building 1, Floor 2).
- This information is entered manually by the customer and transmitted to and stored in U.S. or German regional data centers and U.S. Analytics data center.

Q: How does Proactive Management handle any personal data in Device Data present in the Environment Variables?

A: Environment variables may contain personal names in some of the variable values. Proactive Management software on the device, reads the logged-on Windows user name from the device, and if it is present in the environment variable values, it will remove these before transmitting and storing in U.S. Analytics data center.

However, if a user has provided a user name in the environment variable value that is not the logged-on Windows user name, the Proactive Management software on the device will not be able to remove this before transmitting and storing the environment variable value in the U.S. Analytics data center.

For example, if a user name is John Boe, and the logged-on windows user is jboe, and one of the environment variable value is C:\Users\jboe\Documents, then Proactive Management software on the device will transmit and store this data as C:\Users\username\Documents. However, if the environment variable value is C:\Users\john\Documents, then the Proactive Management software on the device will transmit and store this data as C:\Users\john\Documents in the U.S. Analytics data center.

Q: How does Proactive Management handle any personal data in the Device Data present in the Windows Event Logs?

A: Windows event logs from devices may contain personal data. Because of the volume and variety of the data, it is very difficult to understand, remove and/or sanitize all personal data from Windows event logs data that is transmitted to and stored in the U.S. Analytics data center. Proactive Management does not leverage any personal data from the Windows event logs in its analysis or output.

Data Protection

Q: Is the data transmitted over public networks encrypted using TLS 1.1 or greater, IPsec or other industry standard strong encryption technologies?

A: Proactive Management leverages TLS 1.2 to transmit data between device and the U.S and German regional data centers, the U.S Analytics data center and the U.S. Identity Management data center.

Q: Is data (in databases, logs, configuration files, backup media, etc.) stored securely?

A: All databases in the U.S. and German regional data centers that store personal data are encrypted.

All databases in the U.S. Identity management data centers that store personal data are encrypted.

All databases and unstructured storage in the U.S. Analytics data center are encrypted.

Q: Is personal data (in databases, logs, configuration files, backup media, etc.) stored in clear-text format

A: All databases in the U.S. and German regional data centers that store personal data are encrypted.

Additionally, in the U.S. and German regional data centers, Proactive Management also provides application level encryption and SHA256 hashing for real-time device location data.

Contact data (for personal and/or business including a customer's and/or user's first name, last name, mailing address, telephone number, fax number, email address etc., for Proactive Management accounts) are stored in clear text in the U.S. and German regional data centers, and in the U.S. Identity Management data centers.

Security credentials data (like HP DaaS account passwords) are encrypted in U.S. Identity Management data centers and not stored in clear text.

Q: Is data securely disposed of when no longer needed?

A: All data in U.S. and German regional data centers is deleted permanently within thirty days after customer inactivation from Proactive Management.

Data in U.S. Analytics data center is deleted after five years from the date of data creation
Note: For data protection purposes, all personal data is de-identified prior to transmission to and storage in the U.S. Analytics data center.

Q: How is access to data restricted?

A: All the data collected and stored in U.S. and German regional data centers and in the U.S. Analytics data center is secured by Amazon Web Services (AWS) through IAM roles, authenticated users, and bucket policies.

Q: Does HP DaaS Proactive Management share its data with its HP suppliers, and if so, does it include personal and anonymized information?

A: Yes, Proactive Management shares performance data (disk, CPU, memory) with some of HP's key suppliers for the performance optimization of HP products. HP only provides aggregated and anonymous data without any reference to any HP and/or Proactive Management ustomer.

Q: Does Proactive Management provide separate, dedicated database(s) for customers' exclusive use of their data?

A: No.

Q: Is customer data and information co-hosted with the data from other organizations or companies on the same physical server(s)?

A: Yes.

General Data Protection Regulation (GDPR)

Q: What is GDPR compliance?

A: The General Data Protection Regulation (GDPR) is an European-wide regulation for the protection of European citizens' data that came into force on the 25th of May 2018 and established rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data (Ref: https://gdpr-info.eu/art-1-gdpr/). Currently there is no certification or license required or available for GDPR.

Q: What is HP's and HP DaaS Proactive Management's approach to GDPR?

A: HP has a long-standing history of industry leadership in privacy and data protection. Together with our robust portfolio products and services, we can support our customers' and partners' efforts in protecting personal data. With respect to HP DaaS Proactive Management, HP acts as a Data Processor. Please refer to Data Processor section on HP Privacy Central. As a global company, it is possible that any information you provide may be transferred to or accessed by HP entities worldwide in accordance with the HP Privacy Statement and on the basis of the International Privacy Programs listed in the International Data Transfers section.

Q: Do you have an assigned Data Protection & Privacy Officer or equivalent?

A: Yes, for more information refer to the Frequently Asked Questions (FAQ) in the Data Processor section on HP Privacy Central.

Health Insurance Portability and Accountability Act (HIPAA)

Q: What is the Health Insurance Portability and Accountability Act?

A: The Health Insurance Portability and Accountability Act or HIPAA, is the U.S. law that governs healthcare privacy and contains both privacy and security provisions for safeguarding Protected Health Information.

Q: What is Protected Health Information (PHI) and does HP DaaS Proactive Management collect PHI?

A: Protected Health Information, or PHI, is a defined under U.S. law as any information about health status, provision of health care, or payment for health care that is created or collected by a Covered Entity (or a Business Associate of a Covered Entity) and can be linked to a specific individual. A Covered Entity is one of the following: 1) Health Care Provider (including pharmacies); 2) Health Plan; or 3) Health Care Clearinghouse. A Business Associate is a person or entity that performs certain functions or activities that involve the use or disclosure of PHI on behalf of, or provides services to, a Covered Entity.

HP DaaS Proactive Management software does not collect, store or transmit any information about health status, provision of health care, or payment for health care. However, in certain situations, HP Service Experts may come in contact with such information while performing certain HP DaaS Proactive Management services (for e.g. Remote Support, Device Wipe etc.). Therefore, Account Holder acknowledges that it is solely responsible for its compliance with HIPAA or any other applicable law related to health information. It is the Account Holder's responsibility to verify that the security and privacy protections and storage/retrieval capabilities offered by Proactive Management are adequate and in compliance with all applicable laws

governing the type of data included in the Content which is uploaded into or provided to Proactive Management. In order for HP to provide certain services such as device wiping or remote support, Account Holder may be required, among other things, to identify a remediation plan to achieve HIPAA compliance and/or to enter into a Business Associate Agreement with HP before HP provides such services.

Q: What is a Business Associate Agreement (BAA) and when is one needed?

A: A Business Associate Agreement (BAA) is an agreement between a HIPAA-covered entity and a Business Associate to protect PHI in accordance with HIPAA guidelines.

HP DaaS Proactive Management customers that:

1. Manage all HP DaaS Proactive Management services by themselves do not need to sign the BAA with HP.
2. Leverage HP Service Experts to manage HP DaaS Proactive Management services need to sign the BAA with HP. HP prefers that customers review the HP BAA template or provide their own template before the initiation of any HP DaaS Proactive Management services.
3. Leverage their partners to manage HP DaaS Proactive Management services may want to check with their legal department regarding putting a BAA in place with the partner before the initiation of any HP DaaS Proactive Management services.

4AA7-2191ENW v4 September 18, 2018